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

本书内容简介

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。

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

封面无防伪标均为盗版

“银行业信息化丛书”编委会

主　编：尚福林

副主编：郭利根

编　委：（按姓氏拼音排序）

陈天晴　陈文雄　方合英　甘　煜　谷　澍　侯维栋　李　丹

李　浩　李丽芳　李　翔　李振江　林晓轩　林治洪　潘卫东

庞秀生　曲家文　单继进　童　建　王　兵　王　健　王用生

谢翀达　许　文　薛鹤峰　于富海　张华宇　张依丽　朱鹤新

编　辑：（按姓氏拼音排序）

傅晓阳　龚伟华　何　禹　焦大光　金磐石　李　璠　李海宁

李建军　梁　峰　刘国建　刘秋万　刘子瑞　鲁　森　骆絮飞

吕仲涛　牛新庄　谭　波　汪　航　王　燕　吴永飞　奚力铭

徐　徽　于慧龙　余宣杰　周黎明　周天虹

工作组：（按姓氏拼音排序）

曹文中　陈宇能　黄登玺　黄绍儒　霍宝东　贾俊刚　金建新

李洪伟　李　燕　林长乐　刘文波　孙　莉　唐　宗　卫剑钒

夏建伟　闫晓鹤　张　健　张立书　钟　亮　朱学良

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。

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

第四篇 实 践 篇

第一篇

现状篇

随着我国银行业的发展壮大与信息技术的不断完善，信息安全在银行信息化建设的进程当中扮演着越来越重要的角色。本篇主要讲述了我国银行业及信息技术的发展状况，在此基础上，对我国银行业信息安全的发展现状进行了分析，剖析了我国银行业在信息安全建设上取得的巨大成就。

第 1 章
概述

改革开放以来，我国银行业飞速发展，取得了丰硕的成果，银行业信息化建设经过近三十年的发展，已经打下了坚实的基础，并在当今的互联网时代继续呈现快速发展的势头。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。银行改革与创新的步伐持续加快，金融服务水平和服务能力进一步提高，银行的业务发展越来越依赖信息系统，信息系统安全稳定已经成为银行业务发展的必要保障。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，面对当前和未来金融业的发展需要，银行业在加快信息化发展的同时还要不断加强信息安全的建设，保证银行业务的顺利开展。本章主要讲述了我国银行业发展取得的成就、银行信息技术的发展状况，并对我国银行业信息安全进行了概述。

1.1 我国银行业取得的丰硕成果

改革开放 30 多年来，我国银行业不断探索金融发展模式，逐渐按照银行业客观发展规律进行风险监管，取得了丰硕的成果。30 多年来，在党中央、国务院的正确领导下，我国银行整体实力持续增长，抗风险能力不断增强，公司治理状况明显改善，服务能力和水平日益提升，各类机构协调均衡发展，银行业监管有效性不断提高。

1.1.1 资产增长速度迅猛

根据中国银行业监督管理委员会（以下简称银监会）发布的 2014 年度监管统计数据显示，我国银行业资产和负债规模稳步增长，截至 2014 年 12 月末，我国银行业金融机构境内外本外币资产总额为 172.3 万亿元，同比增长 13.87%。其中，大型商业银行资产总额 71.0 万亿元，占比 41.21%，同比增长 8.25%；股份制商业银行资产总额

31.4 万亿元，占比 18.22%，同比增长 16.50%。

银行业金融机构境内外本外币负债总额为 160.0 万亿元，同比增长 13.35%。其中，大型商业银行负债总额 65.7 万亿元，占比 41.06%，同比增长 7.44%；股份制商业银行负债总额 29.5 万亿元，占比 18.44%，同比增长 16.26%。

1.1.2 国际化步伐加快

在全球经济一体化背景下，商业银行要面对来自全球同行的竞争，我国各银行机构均采取了积极主动的应对策略，通过“走出去”的方式，投入到全球金融竞争的浪潮当中。以中国工商银行为例，通过持续努力和稳健发展，它已经迈入世界领先大银行行列，拥有优质的客户基础、多元的业务结构、强劲的创新能力和市场竞争力。它的业务跨越五大洲，境外网络扩展至 40 个国家和地区，通过 17245 个境内机构、329 个境外机构和 1903 个代理行及网上银行、电话银行和自助银行等分销渠道，向 473.5 万公司客户和 4.32 亿个人客户提供广泛的金融产品和服务，形成了以商业银行为主体，综合化、国际化、信息化的经营格局，继续保持着国内市场的领先地位。2013 年，中国工商银行位列英国《银行家》全球 1000 家大银行榜首，在美国《福布斯》杂志全球企业 2000 强排名中，成为全球最大企业，并首次入选全球系统重要性银行。

截至 2012 年末，中国银行业的境外资产已达到 1 万亿美元，是加入世贸组织前的 6 倍，当年实现利润约 169 亿美元，占总利润的 8.6%，共有 16 家中资银行通过自设、并购、参股等方式在境外设立了 1050 家分支机构，覆盖了亚洲、欧洲、美洲、非洲和大洋洲的 49 个国家和地区。

1.1.3 银行业体制机制改革实现历史性突破

过去我国四大银行都是国有独资银行，而今天，其主要机构已经全部完成股份制市场化改革。这场改革，使得打造资本充足、内控严密、运营安全、服务和效益良好、具有国际竞争力的现代化股份制商业银行的阶段性目标顺利实现。中小商业银行全部完成历史风险化解处置工作，特色化发展、差异化竞争格局逐步形成，部分中小商业银行已经树立起较好的特色品牌。

现代银行在公司治理建设方面已经迈出了重要步伐，“三会一层”的公司治理组织架构已经较为健全。股东依法行使权力履行义务、董事会积极履行“诚信义务”和“看管责任”的体制机制已经初步建立。战略、经营理念及激励约束机制等日渐科学合理化。大多数银行基本实现业务标准化、模块化和流程化管理。部分银行已经开始积极探索实施项目团队积分考核机制，前、中、后台高效协调且有效制衡的组织架构初步建成。

1.1.4 银行业风险管控和抵御能力大幅提升

银行业风险管控能力提升主要体现在以下几个方面：

第一，风险管理制度迈向完备。有关制度规则除覆盖信用风险、市场风险、操作风险三大传统风险之外，更延伸到流动性风险、声誉风险、国别风险、战略风险、法律风险和信息科技风险等领域。资本与风险和信贷增长科学挂钩的机制已基本形成。

第二，现代风险管理技术实现质的飞跃。整个风险管理已从只重表内转向表内外并重和并表核算管理，从关注单一客户的风险转向关注组合风险、控制行业集中度风险，从简单定性判断风险转向定量与定性判断相结合，从主要依靠个人经验转向同时注重专业研判与模型测算。

第三，风险抵补机制建设成效显著。银行机构纷纷高度重视建立科学可行的长期资本补充规划。目前，大型银行通过内部积累和外部融资来补充资本的比例分别约占60%和40%，并积极建立逆周期资本缓冲机制。充分运用形势较好时期的经营成果尽可能核销不良资产，并根据潜在风险变化情况及早计提和调整计提拨备，为未来行为提供明确的指引信号。

第四，风险管理三道防线日趋完善。银行普遍建立了由三道防线组成的风险防控体系。各相关部门是风险管理的第一道防线，是本部门风险的直接承担者和管理者，对本部门风险承担第一责任；具有风险管理职责的风险管理部、法律合规部等部门是风险管理的第二道防线，负责风险管理体系的构建和对全面风险管理的统筹、支持和督促工作；审计部是风险管理的第三道防线，负责对风险管理体系的运行情况进行审计，并依照规定揭示和报告审计过程中发现的问题。三道防线的工作配合日趋成熟和完善。

1.1.5 银行业发展模式发生深刻变化

第一，职能定位回归服务实体经济。近年来，在监管引领下，银行业始终坚持探索支持实体经济平稳健康发展与有效防控风险之间符合客观规律的平衡点；始终坚持探索满足广大人民群众日益丰富的金融需求与加快自身发展方式转变的良性互动机制，始终坚持探索更好地发挥银行业优化社会资源配置、支持经济平稳健康科学发展的路径。对“三农”、小企业、战略性新兴产业等重点领域和薄弱环节的支持力度明显加大，基础金融服务均等化程度显著提高，已经实现全国乡镇基础金融服务的全覆盖。

第二，中间业务取得长足发展。商业银行服务由单一的柜面渠道发展为网上银行、手机银行、移动 POS 等多种渠道，由简单的存贷汇发展为能够开办理财业务、投行业务、托管业务、代理业务、财务顾问、贵金属业务等的金融超市。这使我国银行业主要依靠利差的盈利机制悄然转变。银行业金融机构也更加重视对成本的科学管理和控制，如对资本利润率（ROE）、资产利润率（ROA），以及风险抵扣后的资本回报率（RAROC）和经济附加值（EVA）这些概念，从最初不甚了了到广泛应用于业务和经营的

指导。这为推动银行业金融机构构建向成本要效益、向管理要盈利的长效机制打下了基础。更重要的是，银行中间业务的快速发展，对改变过度依赖利差、单纯地冲规模的传统发展模式，实现战略转型、改革发展正发挥着越来越重要的作用。2010～2013 年，16 家上市银行的中间业务收入复合增长率达到 26.1%，非利息收入平均占比也已超过 20%。

第三，电子银行和移动支付业务发展迅速。根据中国金融认证中心（以下简称 CFCA）发布的《2014 中国电子银行调查报告》，中国电子银行业务连续 5 年呈增长趋势，2014 年个人电子银行用户比例为 43.1%，同比增长 7.2 个百分点。2014 年移动金融势头发展迅猛，移动支付用户比例成倍增长，尤其是远程支付，其 2013 年的用户比例为 13.3%，2014 年达到 37.8%。调查报告显示，2014 年移动支付用户比例成倍上涨，逾五成月支付额为 300～1000 元，此外，近场支付快速发展，我国居民近场支付习惯逐渐养成，月均百元，大多支付 5 次以内，近距离无线通信技术（NFC）近场支付 2013 年的用户比例为 3.6%，2014 年达到 8.5%。调查显示，受手机终端与卡片更换限制，近场支付虽然成倍增长、概念普及度高，但未达到质的突破，应用推广仍有待时日。

2014 年手机银行业务展现出巨大的发展潜力。据《中国电子银行调查报告》预测，2015 年个人手机银行将出现爆发式增长，用户比例将达到 24%，超过 40% 的用户通过手机银行购买理财产品。

2003 年以来，我国的银行纷纷推出各种理财产品。国内商业银行贵宾理财领域的尝试，包括打造顶级的理财团队，为私人客户提供证券、保险、期货、房地产投资甚至律师服务等众多领域的专业理财服务等，为国内私人银行服务奠定了基础。目前我国正积极向金融业混业经营方向靠拢，例如商业银行可以设立基金管理公司、从事 QDII 境外理财业务，保险公司允许设立资产管理公司并可参股和控股商业银行等，这些措施从某种程度上正好迎合了个人对私人银行业务全能化、个性化、复杂化的要求。

随着改革的持续推进，我国银行业的整体规模和竞争力已经实现重大提升。在银行业资产和负债规模方面，2015 年二季度末的数据显示，我国银行业金融机构本外币资产（境内外）总额为 188.5 万亿元，同比增长 12.75%。其中，大型商业银行资产总额为 77.7 万亿元，占比 41.20%，同比增长 9.36%；股份制商业银行资产总额为 35.0 万亿元，占比 18.59%，同比增长 15.07%。银行业金融机构本外币负债（境内外）总额为 175.2 万亿元，同比增长 12.20%。其中，大型商业银行负债总额为 72.1 万亿元，占比 41.14%，同比增长 8.68%；股份制商业银行负债总额为 32.9 万亿元，占比 18.78%，同比增长 14.66%。

1.2 信息技术在我国银行业的发展

伴随着改革和对外开放，我国金融业信息化建设从无到有，取得了令人瞩目的成就，已经成为决定我国金融业发展和提高金融竞争力的关键因素之一。随着我国经济的

不断发展，各商业银行基本完成了数据全国集中处理（称为“数据大集中”），进一步建设完善了新一代核心业务应用处理系统。银行金融服务创新加快，服务水平进一步提高。重要的标志是银行卡的应用和网上金融服务的迅速发展。现代银行业作为知识密集型产业，与传统银行业相比，在组织结构、业务流程和业务开拓等方面，日益体现出以知识和信息为基础的特征。银行业的这种行业属性，决定了其必须以飞速发展的信息技术为支撑。

1.2.1 商业银行信息科技发展阶段

我国商业银行信息科技发展大致经历了四个阶段。

第一阶段是20世纪70年代末～80年代中期的单机批处理阶段。这一阶段是银行信息化建设的起步阶段，银行的储蓄、对公等业务逐渐以计算机处理代替手工操作，本阶段的系统特点主要体现为按照业务网点分散建设、单机操作，只是用计算机取代了算盘和手工账簿。1974年，中国银行香港分行成立并组建了电脑中心，该电脑中心是我国把信息技术应用到银行业的第一个大型计算中心，从此，我国金融行业开始了IBM大型主机系统的使用。使用计算机系统进行单机批处理业务的成功实践，标志着我国银行业信息化开始建立。

第二阶段是从20世纪80年代中期～90年代末期的联机网络阶段，这一阶段银行开始通过使用计算机网络技术实现部分业务的实时联机处理，并逐步实现了在一定区域范围内的数据集中及互联互通。区域集中让所辖银行得以共享数据资源，统一了科目设置，改进了业务流程，提高了服务质量。这一阶段开始出现国产化软件。

第三阶段是从1995年开始的“数据大集中”阶段，这一阶段在第二代系统基础上对业务管理流程进行变革，全国性的银行数据通信网络框架基本建成，各银行的综合业务处理网络相继建成，提出了大会计与综合柜员制的概念，一个多功能的、开放的银行信息化体系初步形成，全国性的数据大集中让银行的数据在更大范围内共享，数据的收集和管理更加方便，管理和决策也更加高效便捷。

1999年，中国工商银行正式启动“数据大集中”工程，将该行的主要业务集中到北京、上海两大数据中心处理。2002年，两大中心数据的成功挂接，在我国银行信息化发展历程中具有里程碑式的深远意义。

第四阶段是从2000年左右直到现在的互联网阶段。随着互联网和其他数据网络的爆炸式增长，引发了一场全球性的商务革命和经营革命。每个电子交易都需要经过资金的支付与结算才能完成，而作为资金流负载者，银行的参与是至关重要的。因此，随着互联网的发展，网上银行服务也蓬勃发展起来。为了能取得成功，银行必须借助互联网的力量，并使之同计算机与通信技术、信息技术结合起来。网上银行伴随着云计算、大数据、移动互联、在线支付等新型服务渠道不断涌现，我国银行业信息化发展步入了一个新的时代。

1.2.2 信息技术对银行发展的重要意义

银行业的高度信息化和知识化，使服务前台和管理机构的信息能够实时传送到决策部门，实现智能化决策和快速反应，从而大大提高管理效率，扩大管理范围，减少管理层次，促进银行的管理模式向“扁平化”方向转变。

信息化帮助银行实现以客户为中心的业务流程再造。信息化帮助银行从根本上重新思考和设计现有的业务流程。根据客户类别，将分散在各职能部门的工作，按照最有利于顾客价值创造的营运流程进行重组，使银行能有效适应市场的要求，从而建立“客户中心型”的流程组织，以期在成本、质量、顾客满意和反应速度等方面有所突破，进而在财务绩效指标与业绩成长方面有优异的表现。

信息化已成为金融工具创新的主要源泉。在业务开拓方面，信息化已成为金融业增长的源泉因素，信息系统的服务已经涵盖了银行所有的核心业务流程。新的金融工具和服务方式的推行，往往是金融性质的市场行为同信息技术相互耦合的结果，信息化为金融市场的参与者提供了充足的信息和基于知识的量化评价，辅助了决策行为，使金融产品的交易更为简单，从而扩大了金融市场。

1.2.3 信息技术在银行业中的应用前景

银行业信息技术发展是涉及银行各类资源整合和银行所有利用互联网、无线技术、电话等信息技术手段进行电子化交易、电子化信息沟通、电子化管理的活动，贯穿公司经营管理的全过程。银行业信息技术是随着互联网技术兴起逐渐成熟的，新的信息技术在金融公司内又一轮深层次的商务应用，是信息技术本身和基于信息技术所包含、所带来的知识、技术、商业模式等在银行内的扩散和创新。拓展信息技术在金融行业各个领域的应用，利用信息技术发展金融企业的商业模式将是银行业未来发展的主要方向。

由于全球金融危机的出现，未来全球金融领域将面临一场挑战，在应对危机的同时要面对信息化和金融全球化的浪潮。为此，我国银行业应积极准备，精心策划，利用互联网进行金融产品的宣传和销售，提供全方位的金融服务活动，并通过互联网加强与国内外金融公司的业务往来和经验交流。我们相信，全方面发展信息技术，有利于推动我国金融行业的长足发展，使之以全新的姿态积极参与国际金融市场的竞争。

1.2.4 信息技术在银行业中的主要作用

信息技术增强了银行的内部管理能力。

① 信息技术有助于银行快速方便地获取外部环境信息，及时分析银行所面临的机会与威胁，实现战略制定、调整与转移。

② 信息技术提供给管理者多种形式的运营信息、外部行业信息、国家经济政策信息，既加强了决策的有效性，又提高了管理者的工作效率。各方面信息提供及决策支持技术的发展弱化了银行高层领导依赖下属进行评价和建议的程度，提高了决策的质量。

③ 信息技术改善了沟通方法、下放了决策权、加强了工作的计划性，因而可以大幅度地扩大管理辖幅、增强决策的透明度、缓解时间的压力、减少事故发生与发现之间的延误。

④ 信息技术方便了人力资源管理，对于加强对员工的培训，提高员工技能有重要的作用。

信息技术对于提高银行的竞争力具有重要作用。信息技术服务于银行业务的态势日益明显。在服务中通过信息技术挖掘和发现潜在的业务需求，提高对新兴业务的认知度，支持银行业务全面发展，争取到更多、更优质的客户群体，使信息技术工作在公司业务、个人业务、电子银行、中间业务等领域不断创新，信息技术向业务部门的渗透力和转化力不断加强，从而提升银行的核心竞争力。

信息技术对银行业日益显现出变革性的影响。信息技术的迅猛发展对银行业的影响已不限于业务处理方式和工具，而是演变为推动银行业变革的主要力量。根植在现代信息技术之上的现代银行业，其快速发展需要相应的智能化金融基础设施体系与之配套，包括建立智能化的支付清算体系，在加快资金周转的同时有效防范支付风险；建立智能化的信息平台、终端技术和数据存储体系，提高数据挖掘能力和效率；建立智能化的机构和网点，实现业务管理和运作的智能化；建立智能化的监管体系，实现更大范围和更有效的监管。

1.2.5 我国银行业信息化建设发展进入快车道

我国银行业信息化建设取得巨大成就，未来仍将继续快速发展。

1. 金融信息基础设施日趋完善

我国金融业拥有世界先进水平的大型计算机、小型计算机、PC 服务器、刀片服务器等各类计算机，建立了覆盖全国的网络通信系统，开发了大量金融信息和业务处理系统，形成了比较完整的金融信息基础设施体系。

2. 数据集中工程基本完成

以国有商业银行为代表的各金融机构实现了业务数据的集中处理，统一、规范了业务操作流程，重新设计了营运流程。建立了集中式的数据中心，有效提高了数据处理能力和整体可靠性，为管理信息系统提供了基础数据，为下一步实现经营集约化、管理信息化、决策智能化奠定了基础。

3. 新一代核心业务系统成功投产

在银行核心业务系统进入数据大集中阶段后，各家银行对新一代核心业务系统建设和改造有诸多共性的特点：更加强调以客户为中心，在行内统一客户视图，满足客户个

性化金融服务需求；更加强调产品快速开发能力，通过灵活技术应用架构设计，提升对市场需求的响应速度；更加重视业务模型和数据模型，以适应金融发展改革带来的精细化经营管理需求。当然，各商业银行核心业务系统的差异性较大，其业务范围、设计理念、技术路线和建设方式各有不同，各行的业务连续性、信息科技治理能力、信息安全保障水平也有所不同。

1.2.6 未来几年我国银行业信息技术发展的趋势

1. 加强信息科技治理，提高信息化管理水平

未来几年，银行业要建立起适应数据大集中技术环境和银行组织变革要求的信息组织体系，合理配置科技资源，努力构建面向业务、服务导向、分工合理、协作紧密、运作高效的专业信息化组织架构。

要建立信息科技战略和计划的流程，保证信息科技战略与企业战略的一致性，确保信息科技技术投资决策符合本行远景。建立统一的项目管控组织和制度流程，加强项目协调和管控，加强需求、方案设计、投产验证等关键阶段的管理，确保项目过程的有效控制。建立统一的信息科技策略，推进企业信息科技技术标准化，统一信息科技架构、规范信息科技技术采用，提高效率、降低成本。进一步完善供应商管理机制，加强供应商的有效控制，为银行信息化发展提供安全高效的外部资源支持。

在完善信息科技运行管理的基础上，建立和完善服务级别管理、可用性管理等流程。尝试建立信息科技财务管理流程和标准化的信息科技服务水平协议，实现服务交付，提升和展示信息科技服务的价值，努力实现银行信息科技运营管理从以技术为中心的管理阶段向以服务为中心的管理阶段转变，降低信息化总体拥有成本。

2. 建立“以客户为中心”的金融产品和服务渠道体系，提高银行服务水平

大力加强基于信息技术的金融创新，提高产品创新能力，实现由“以产品为中心”向“以客户为中心”的转变。采用先进灵活的应用体系架构，加快应用整合，支持业务流程再造，缩短系统开发周期，提高产品交付能力。进一步完善、拓展银行的服务渠道，提供方便、快捷、个性化的客户服务。加快渠道整合步伐，实现产品“一次开发，多渠道部署”，以降低开发及部署成本、加快产品投产速度、提高客户满意度、增强市场竞争力。

3. 完善银行业信息安全应急恢复体系，加强灾备中心的建设，保证系统的安全稳定运行

加强安全监控，进一步完善信息安全应急处置机制和信息通报机制，制定应急预案并进行演练，明显提升金融信息系统预警、应急处置和恢复能力，保障金融业务的连续稳定运行。探讨建立银行业应急救援中心的可行性，加大应急技术支持和救

援力度，加快业务的恢复速度，并最大限度地实现资源共享，推动传统银行向流程银行转变。

4. 推动传统银行向流程银行转变

面对互联网金融、利率市场化等多种外部环境的变化，商业银行必须加强自身的管理创新、业务创新、流程创新，以适应新的市场竞争环境。摆脱传统银行模式中过于精细的劳动分工羁绊，使银行的组织形式向扁平化、精益化的方向发展。从生产或产品导向转变为消费者导向和服务导向，突出核心业务流程和业务流程的多样化，通过业务流程的再造来引发组织流程和管理流程的再造，从而推动传统银行向流程银行的转变。

5. 加强信息科技风险管理，完善研发运维体系

信息科技风险管理一直是银行的一项重要任务。未来商业银行应着力加强培育信息科技风险管理文化，优化组织架构，制定信息科技风险管理战略、政策、制度、流程、方法，提高组合风险管理水平，将信息科技风险管理纳入到全面风险管理体系中；把风险管控贯穿于信息系统生命周期，建立起信息科技风险管控的日常化、流程化、持续化机制。

1.3 银行业信息安全概述

1.3.1 信息安全重要性日益凸显

信息技术在银行业中的广泛应用，大大提高了银行资源的使用效率和人员的工作效率，增加了银行的核心竞争力。但在银行信息科技发展的过程中，信息技术的安全隐患也越发突显出来，如自然灾害、数据泄露、病毒攻击、人员操作失误等。如何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，逐渐成为银行信息技术发展的一个重要课题。

1.3.2 信息安全在银行业中的发展阶段

银行业信息安全的发展大致可以分为 3 个阶段：

第一阶段：从 20 世纪 70 年代后期至 80 年代初期的银行电子化阶段。该阶段银行应用系统封闭，面临的威胁较小，主要通过内控、安全审计等方法进行信息安全控制。

第二阶段：从 20 世纪 80 年代至 2000 年左右的信息科技优化阶段。在这个时期主要通过防火墙、入侵检测系统、漏洞修复、系统扫描等多种手段形成纵深防御体系，客户端采用强密码学方法，通过硬件密码产品，逐步形成金融生态圈的安全体系。

第三阶段：从 2000 年至现在的信息科技价值创造阶段。随着互联网应用加强，手机等智能终端普及，信息安全面临新的挑战，银行业通过国密算法、金融 IC 卡、国产

芯片、应用程序安全开发、安全协议等各种方法，面对新形势加强了对信息安全的建设。

40 多年来，我国银行业信息安全建设从无到有，取得了令人瞩目的成就，已经逐渐成为决定我国银行业发展和提高金融竞争力的关键因素之一。

1.3.3 信息安全是银行业永久性的话题

就银行业而言，几乎所有的业务都运行在信息技术基础设施之上，尤其是新出现的金融产品和服务更加趋于开放和互联，进一步加强了对信息系统的依赖程度。

信息系统和信息安全已经成为操作风险管理的重要内容。信息的保密性、完整性、有效性及信息系统可用性对银行业务的成败起着至关重要的作用。

银行业信息系统在规划、研发、建设、运行、维护、监控及退出过程中，由于技术和管理缺陷容易产生操作、法律和声誉等风险，而信息安全在银行业中具有技术性高、涉及范围广、隐蔽性强等特征。

随着攻击者的泛滥，商业银行业面临着信息安全挑战。首先是技术问题，表现为计算机硬件、软件、网络及相应业务信息系统所引发的异常情况，包括程序错误、系统宕机、软件缺陷、操作失误、硬件故障、容量不足、网络漏洞、故障恢复灾难备份及应急处理等诸多内容。其次是管理问题，不仅包括信息系统的管理，而且包括商业银行各种业务数据的管理。

信息安全是银行业永久性的话题。银行应用系统相互牵连、使用对象多样化、安全风险多方位、信息可靠性、保密性要求高等特征构成了银行系统的突出特点。国际金融危机以来，银行系统的风险控制和监管被提到了前所未有的高度。如何利用信息技术的优势加强银行机构的内部控制，提高金融监管和服务水平，防范和化解金融风险，促进金融改革和创新，从而推动我国经济社会的发展，是当前我国银行业信息化建设面临的重大问题。

第 2 章
银行业信息安全发展现状

信息系统是银行业务正常运行的重要支撑平台，如果信息系统出现了故障或受到攻击，可能导致一个银行的局部甚至整体瘫痪。随着信息技术的飞速发展和国际上网络冲突的不断加深，银行信息系统面临着越来越多的安全威胁。信息系统安全已经成为关系到银行业务能否顺利开展的重要因素，因此必须确保银行业信息安全得到保障。近年来，我国银行十分重视信息安全建设，并取得了卓越的成效，为我国银行业快速发展做出了巨大的贡献。

本章描述了信息安全的定义、范围，对我国银行业面临的威胁和信息安全建设取得的成绩进行了阐述和分析。

2.1 信息安全含义及范围

信息安全本身包括的范围很大，其中包括如何防范商业企业机密泄露、防范不良信息的泛滥、个人信息的泄露等，也包括网络安全、系统安全、各种安全协议、安全机制（数字签名、消息认证、数据加密等）等内容。通过信息安全工作，确保信息系统（包括硬件、软件、数据、人、物理环境及其基础设施）受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，信息服务不中断，最终实现业务的连续性。

信息安全的含义在不断延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性等，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。总的来说，信息安全主要包括以下七方面的内容，即需保证信息的机密性、完整性、可用性、真实性、可核查性、不可否认性、可靠性。

1）机密性（Confidentiality）：信息不能被未授权的个人、实体或者过程利用或知悉的特性。

2）完整性（Integrity）：保护资产的准确和完整的特性。

3）可用性（Availability）：根据授权实体的要求可访问和利用的特性。

4）真实性（Authenticity）：确保主体或资源与它们声称相一致的特性。真实性可应用于诸如用户、进程、系统及信息等实体。

5）可核查性（Accountability）：确保实体的活动可以唯一追溯到该实体的特性。

6）不可否认性（Non-repudiation）：确信实体活动发生或未发生的特性。

7）可靠性（Reliability）：预期的行为和结果的一致性。

信息安全是一个综合、交叉的学科领域，它综合利用数学、物理、通信和计算机等诸多学科的长期知识积累和最新发展成果，进行自主创新研究，加强顶层设计，提出系统的、完整的、协同的解决方案。与其他学科相比，信息安全的研究更强调自主性和创新性。自主性可以避免后门，增强安全可控；而创新性可以抵抗各种攻击，适应技术未来发展。

2.2 银行业面临的威胁分析

2.2.1 银行业面临的攻击威胁

银行业网络及信息系统作为我国关键基础设施的重要组成部分，其安全稳定运行关乎人民群众的切身利益，关系到金融稳定和社会稳定的大局。根据银行业的业务和信息系统特点，可以将银行业面临的威胁描述如下：

（1）资金盗取 如银行卡盗刷、网上银行账户被盗等。

（2）业务欺骗 某一伪系统或系统部件欺骗合法的用户或系统自愿地放弃敏感信息等。

（3）信息泄露 信息被泄露或透露给某个非授权的实体。

（4）网络诈骗 以非法占有为目的，利用互联网采用虚构事实或者隐瞒真相的方法，骗取数额较大的公私财物的行为。

（5）破坏信息的完整性 数据被非授权地进行增删、修改或破坏而受到损失。

（6）拒绝服务 对信息或其他资源的合法访问被无条件地阻止。

（7）非法使用（非授权访问） 某一资源被某个非授权的人或以非授权的方式使用。

（8）窃听 用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。例如，对通信线路中传输的信号搭线监听，或者利用通信设备在工作过程中产生的电磁泄漏截取有用信息等。

（9）业务流分析 通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

（10）假冒 通过欺骗通信系统（或用户）达到非法用户冒充合法用户，或者特权小的用户冒充特权大的用户的目的。黑客大多采用假冒攻击。

（11）旁路控制 攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。例如，攻击者通过各种攻击手段发现原本应保密，但是却又暴露出来的一些系统“特性”，利用这些“特性”，攻击者可以绕过防线守卫者侵入系统的内部。

（12）越权 被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他非授权的目的，也称作“内部攻击”。

（13）网络攻击 黑客通过网络对银行进行攻击，造成银行网络、系统瘫痪，数据被盗和丢失等。

（14）特洛伊木马 软件中含有一个觉察不出的有害程序段，当它被执行时，会破坏用户的安全。这种应用程序称为特洛伊木马（Trojan Horse）。

（15）陷阱门 在某个系统或某个部件中设置的“机关”，使得在特定的数据输入时，允许输入者违反安全策略。

（16）计算机病毒 一种在计算机系统运行过程中能够实现传染和侵害功能的程序。

（17）人员不慎 一个授权的人为了某种利益，或由于粗心，将信息泄露给一个非授权的人。

（18）媒体废弃 信息被从废弃的磁碟或打印过的存储介质中获得。

（19）物理侵入 侵入者绕过物理控制而获得对系统的访问。

（20）安全系统疏于维护 因为金融行业一般都较早地进行了信息化建设和维护，很多时候做过周密的预案和灾备演练后就放松了对系统的整体安全维护。

近年来，针对银行业的网络攻击相当猖獗，恶意软件、病毒及钓鱼网站层出不穷，利用银行信息系统或银行卡进行的资金盗取、业务欺骗也时有发生，成为银行信息安全防护的重点。

同时，我国银行业信息系统和网络的自主控制能力仍然不强，核心关键领域还是依赖于某些厂家的产品和服务，缺乏判断设备是否存在“后门”“软件缺陷”“软件炸弹”等安全隐患的能力。

2.2.2 银行信息安全风险成因

1. 信息系统本身固有的风险

信息化在推动银行发展的同时，也给银行自身带来了巨大的风险，由于信息化规模的不断扩大，信息技术迅速发展，银行信息系统所采用的信息科技技术与信息系统软硬件本身存在着大量的弱点，这些弱点被特定的威胁利用，就会产生风险，从而对银行信息系统的机密性、完整性及可用性产生损害。信息化程度越高，风险就会越大。例如，系统漏洞、硬件故障、意外灾祸都会造成银行信息系统不能正常工作，从而造成重大问题。

2. 银行数据集中处理的风险

银行数据大集中是银行发展的必然趋势，只有完成数据集中，才能实现银行账务数据与营业机构的分离，为银行管理集中和科学运营奠定基础，帮助银行从以账务和产品为中心转变为以客户为中心。但是，数据集中有其有利的一面，也有不利的一面，集中后信息系统风险增大，系统一旦出现问题，出现数据泄露等情况，不但会影响到整个银行的正常运营，还会影响银行的声誉，造成不可估量的损失。

3. 网络金融服务信息安全风险

近年来，网络金融服务，如网上银行、移动银行、电子商务结算等，出现暴发性的增长，已成为目前国际范围内成长最为迅速的银行业务品种，也是银行争相追逐的利润增长点。其中绝大部分的 B2B、B2C 业务要通过互联网、无线网、电话网与银行相连。银行业务系统要顺应开放和互连的趋势，其信息安全范畴已经突破了以业务系统物理隔离和协议隔离为基础的传统银行信息安全，如何在公网环境下防止黑客和病毒的破坏，如何在危机四伏的互联网上保证支付系统的安全性，是银行信息系统面临的挑战。

4. 人为造成的风险

统计结果表明，在所有的信息安全事件中，只有 20% ~30% 是由于黑客入侵或其他外部原因造成的，70% ~80% 是由于内部员工的疏忽或有意泄密造成的，人的因素比信息安全技术和产品的因素更重要。因此人为信息安全风险至关重要。银行业作为信息安全领先行业，在这个方面考虑慎多，对于认为造成的风险从制度、员工意识及各种控制措施等多个方面进行了有效防范。但是安全没有止境，在信息安全问题上，银行业要以人为本，而内部完备的安全管理政策、安全教育计划与健全的银行安全文化建设也成了非常重要的工作。

总的来讲，面对形形色色，种类繁多的各种威胁和风险，我国银行业在信息安全建设方面做了大量的工作，取得了卓越的成效。

2.3 银行业信息安全政策的制定与监管趋于完善

信息安全在我国银行业及其他各行各业的地位越来越高，国家和行业层面也加大了指导和监管力度。从我国来看，国家安全委员会、网络安全和信息化领导小组及其办公室、国务院、中国人民银行（图 2-1）、银监会及中国信息安全测评中心、中国信息安全认证中心、国家密码管理局等机构从不同角度对信息安全制定和提出了相关的政策和要求。

2014 年 1 月 24 日，中央国家安全委员会成立。中央国家安全委员会作为中央关于国家安全工作的决策和议事协调机构，向中央政治局、中央政治局常务委员会负责，统筹协调涉及国家安全的重大事项和重要工作。我国处在经济结构转型的阶段，信息化在转型过程中作用至关重要。国安委的成立，标志着信息安全战略已经成为国家安全战略

的重要组成部分，在国家安全建设中占据重要地位。

2014 年 2 月 27 日，中央网络安全和信息化领导小组成立。领导小组将着眼于国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。

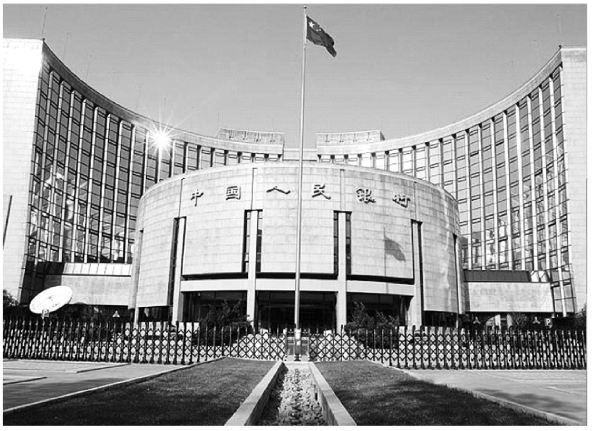


图 2-1　中国人民银行

公安部为了规范信息安全等级保护管理，于 2003 年 7 月成立了公安部信息安全等级保护评测中心，为国家管理部门在推进信息安全等级保护工作过程中的监督、检查、指导等行政执法工作提供专业技术支持，对国家基础网络和重点信息系统的安全保护状况进行权威测评并提出改进建议，负责全国信息安全等级测评体系和技术支撑体系建设的技术管理及技术指导。2007 年，公安部依据《中华人民共和国计算机信息系统安全保护条例》，经法律授权，会同国家保密局、国家密码管理局和原国务院信息办共同发行了《信息安全等级保护管理办法》，对信息安全保护等级做出了明确的规定，为指导各地区、各部门开展等级保护工作提供了政策保障。

国家密码管理局为了促进我国信息科技健康有序的发展，发布了《电子认证服务密码管理办法》《证书认证系统密码及其相关安全技术规范》等规章制度和《国密 SM1》《国密 SM2》《国密 SM3》等密码算法。2012 年，国家密码管理局发布公告，批准《祖冲之序列密码算法》《SM4 分组密码算法》等六项密码行业标准，用于对不涉及国家秘密内容但又具有敏感性的内部信息、行政事务信息、经济信息等进行加密保护。

中国人民银行对于银行业信息科技的发展非常重视，早在 2002 年，中国人民银行就发布了《银行计算机安全事件报告管理制度》来保障银行计算机安全管理，防范信息系统的技术缝隙，保证银行信息系统的安全运行。

2006 年，中国人民银行发布《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》，对建立和完善与银行业金融机构信息化发展相适应的信息安全保障体系，满足银行业金融机构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，显著提高银行业金融机构的业务持续运行保障水平提出了要求。

现阶段中国人民银行认真贯彻中央经济金融工作大政方针和决策部署，主动适应金融改革开放新形势，积极履行科技管理和服务职能，各项工作取得了新进展，包括制定金融业网络安全规划，组建信息安全专控队伍，启动央行应急监控指挥中心和灾备中心建设，加强数据中心风险防控，发布银行业标准化工作指南，建立央行信息技术标准体系，完善金融业检测认证基础设施，全面推进金融机构代码应用，建成我国全球法人识别码（LEI）本地注册渠道并实现国际互认，关闭金融 IC 卡降级交易，推进移动金融安全可信服务平台应用和创新试点工作等，为推动我国金融改革发展、维护金融稳定、促进金融服务社会民生等方面提供了重要的技术支撑。

针对银行业监管标准，银监会（图2-2）于2009年发布了《商业银行信息科技风险管理指引》，替代了2006年发布的《银行业金融机构信息系统风险管理指引》。新发布的《商业银行信息科技风险管理指引》具有以下几个特点：①全面涵盖商业银行的信息科技活动，进一步明确信息科技与银行业务的关系，对于认识和防范风险具有更加积极的作用。②适用范围由银行业金融机构变为法人商业银行，其他银行业金融机构参照执行。③信息科技治理作为首要内容提出，充实并细化了对商业银行在治理层面的具体要求；④重点阐述了信息科技风险管理和内外部审计要求，特别是要求审计贯穿信息科技活动的整个过程之中。⑤参照国际、国内的标准和成功实践，对商业银行信息科技整个生命周期内的信息安全、业务连续性管理和外包等方面提出高标准和高要求，使操作性更强。⑥加强了对客户信息保护的要求。

图 2-2　中国银行业监督管理委员会

为加强商业银行数据中心风险管理，银监会还于2010年发布了《商业银行数据中心监管指引》对我国商业银行设立与变更、风险管理、运行环境、运营维护、监督管理等方面做出了要求，保障数据中心安全、可靠、稳定运行，提高商业银行的业务连续性水平。

银监会于2012年8月5日对外宣布，经中央机构编制委员会办公室批准，设立信息科技监管部。该部门的主要职责是制定银行业信息科技监管政策，指导银行业信息科技发展规划，开展信息科技非现场监管和现场检查，处置信息科技突发事件，开展银行业标准化相关工作及银监会信息科技风险防范工作归口管理。其被赋予的使命是加强银行业信息科技监管督导和专项排查工作，维护银行业稳健运行。银监会系统要进一步强化银行业信息科技风险监管工作，加强信息科技风险的监测和预警，深入开展信息科技现场检查，做到风险早发现、早报告、早处置，进一步提升信息科技风险监管的及时

性、前瞻性。此外，银监会还要求银行业金融机构做到风险排查到位、管理措施到位、整改落实到位，要从维护银行业稳健运行的全局出发，加强银行业信息科技监管督导和专项排查，督促提高信息系统的可靠性和稳定性。

2013 年 9 月，银监会发布了《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》（39 号文），明确将安全可控信息技术应用纳入战略规划，预计到 2019 年，安全可控信息技术在银行业使用率总体达到 75% 左右。

当前，银监会推动银行业“安全可控”技术应用的重点在于网络设备、存储、中低端服务器、信息安全、运维服务、文字处理软件，并将在操作系统、数据库等领域加大力度。根据上述 39 号文，从 2015 年起，银行业金融机构对安全可控信息技术的应用应以不低于 15% 的比例逐年增加，直至 2019 年达到不低于 75% 的总体占比。39 号文中部分量化指标将纳入各行 2015 年年度考核，包括安全可控信息技术每年不低于 15% 的增加率。另外，从 2015 年起，银行业机构应安排不低于 5% 的年度信息化预算，用于支持围绕安全可控信息系统的研究。

2.4 银行业在信息安全建设方面取得的卓越成效

2.4.1 明确信息安全管理目标和策略，完善信息安全制度体系

我国各商业银行均十分注重整体信息安全管理策略建设。遵循监管要求，结合自身实际，银行确立了全行信息安全管理目标：一是有效保护信息及信息处理环境，支持业务持续运营；二是提高应对新型信息安全威胁的能力，支持业务创新；三是保护客户信息和资金安全，维护银行声誉；四是提高合规管理能力，满足监管要求。制定了“全面管理、预防为主、分级保护、合规审慎”的信息安全管理原则，确定了信息资产的等级划分策略，明确了对不同等级信息资产的信息安全管理偏好，为信息安全管理指明了方向。

在信息安全管理策略的指引下，银行结合信息科技检查及内外部审计意见，组织完善了信息安全制度框架体系，按照“全面防范，重点突出”的原则，先后制定发布了一系列涉及物理安全、网络安全、系统安全、桌面安全、应用安全、数据安全、开发安全、运行安全、风险评估、风险处置和应急管理、信息科技审计等方面的信息安全管理制度。具体内容包括：按照银监会《商业银行信息科技风险管理指引》，组织制定了配套的信息安全和业务连续性管理的政策、管理办法、操作规范和指南，构建了全行信息安全管理整体框架，明确了信息安全管理对象、管理角色及各对象全生命周期的安全管理要求，规范运维中的安全管理行为；统一全行安全评估的尺度和方法；明确应急管理要求，实行信息系统责任事故的责任认定，在员工行为准则中明确了违反信息科技管理原则的处罚办法。

通过上述工作，我国银行业初步建立了以政策、制度、标准为导向的信息安全管理

体系，建立了涵盖开发、运维、合规、治理全方位的信息安全管理制度体系。

2.4.2 以国家等级保护要求为指导，构建信息安全技术保障体系

我国各商业银行都全面落实了国家信息系统安全等级保护要求，根据国家信息安全等级划分标准，制定信息系统安全技术基线，明确了不同安全等级信息系统的安全保护要求，编写了信息系统安全技术选用指南，明确了实现信息系统安全要求的技术方法，编写了信息系统安全产品选用指南，明确了信息技术所需安全产品的选用原则，从而建立了从需求、安全设计到安全实现的整体安全建设流程。

1）构建了信息系统安全技术架构，明确了信息系统共有安全技术基础平台的建设原则，明确了信息系统建设中使用基础平台的策略，为安全技术整合、优化提供了方向，为银行信息系统安全技术应用提供了指导原则。目前，已采用共性任务集中建设的策略构建银行性安全基础平台。统一开发了用户认证授权管理平台，面向银行网络、系统和应用提供统一身份认证和权限控制服务；统一开发了加密安全管理平台，为各应用系统提供加密服务；银行引进部署了数据安全传递和安全销毁工具，为银行重要生产数据提供覆盖全生命周期的统一安全策略、数据访问控制和数据防泄露等服务；在应用系统运维管理方面，建设运维安全管理平台、日志管理与安全事件监控系统，提供统一的运维操作授权、监控和审计等服务。

2）遵循等级化安全技术架构，银行采用纵深防御的策略构建信息运维安全保障体系，与电信、公安等部门建立协防机制，借助国家力量防范恶性及大规模攻击行为；统一规划互联网、外联网安全防护标准，部署防火墙、入侵检测系统、信息过滤系统、行为检测系统，防范边界风险隐患；加强网上银行安全威胁发展趋势的跟踪、分析和研究，推动新技术新产品在网上银行等互联网系统中的应用，加强安全渗透测试和假冒银行网站的检测；合理划分内部网络区域，有效隔离生产网、办公网和测试网；统一部署构建桌面安全防护体系，为银行计算机终端提供统一的病毒防范和漏洞补丁管理等服务。推进作业调度系统，改变通过手工或系统命令调度的方式，建设自动化运维管理平台，实现日常信息科技运维中重复性工作“自动化、集约化、规范化”，避免人为操作带来的安全隐患，建立运维监控系统，实现系统设备全方面动态监控。

3）采用全生命周期管理策略构建软件安全开发体系，建立软件安全需求识别模型和需求审核机制，把好软件安全需求审核关；制定软件安全编码指南，引入软件代码安全扫描工具，把好软件研制关；引入 Web 应用系统等渗透测试工具，建立软件安全测试流程和渗透扫描机制，把好软件上线管理关。

通过上述安全措施，各商业银行均初步建立了涵盖软件开发安全、运维安全的技术保障体系。

2.4.3 借鉴国际标准，完善信息安全开发和运维

在系统安全开发和运维管理流程方面，银行已经对项目开发管理的可行性研究、需

求分析、立项评审、编码安全、测试、投产上线等全过程进行了规范管理。在项目立项环节，加强了方案的架构审核和安全评审，严格执行信息安全技术架构原则。在软件开发环节，大力推广使用代码检测技术和漏洞测试工具，提高软件编码质量，防范软件开发过程中存在的风险和漏洞。在测试管理上，成立了测试团队，负责跨系统的连接测试、集成的功能和性能测试及上线版本检验测试，并对网上银行等重点系统开展安全渗透性测试。在投产上线前，强化上线集中审核制度，加强上线前的审核和控制，防范上线过程中和上线后出现的系统运行风险。

银行还全面深入开展运行精细化管理，加强系统运维计划管理。推广 ITIL 管理流程，对系统运维工作进行全面梳理，明确主要问题和薄弱环节，部署系统运维计划管理系统，加强变更操作过程控制，完善变更审核流程等措施，控制变更操作风险；制定系统数据备份策略，建立备份数据验证环境，提高数据安全保障能力；细化系统运行事件分类，建立事件处理知识库，提高运行事件响应处理能力；优化岗位设置，细化岗位职责、报告路线、任职资格和绩效考核指标，不断提高运维人员的工作责任心。

2.4.4 持续开展信息安全管理文化建设，提高全员安全意识和安全技能

人是信息安全管理中最重要的因素，银行始终坚持员工合规管理和安全培训两手抓。加强合规管理，以流程管理引导员工做正确的事，以严格制度促使员工规避风险。加强信息安全知识培训，培训开发人员安全编码能力，提高软件安全质量；编印员工信息安全知识手册、信息安全实务手册及相关课件，开展全行信息安全知识竞赛，传递信息安全基础知识和基础技能，提高员工安全应用信息系统的能力；加强银监会风险提示宣传和内部风险警示教育，以典型事件教育、提升全员信息安全意识，以常规化的培训教育，促进信息安全管理文化的建设，营造“人人参与，全员共进”的良好信息安全管理氛围，保障银行信息系统的安全运营。

2.4.5 全面提升信息科技内控水平

针对信息科技风险，银监会于 2009 年颁布了《商业银行信息科技风险管理指引》，其中对我国银行信息科技治理、信息科技风险管理、信息安全、内外部审计等方面做出了规定，保证银行信息技术（系统）安全、持续、稳健地运行。

系统复杂性、过度依赖外包及制度执行力不足是影响信息科技内控能力的关键因素，银行应从加强架构管控和系统整合、加强自主运维和自主开发、加强信息科技检查等方面控制上述不利因素，全面提升信息科技内控能力。

1. 加强架构管控和系统整合

银行从发展战略的高度，依据信息科技规划、架构标准及现有的资源和能力，不断

强化企业级架构的管控，规划、设计了企业级应用架构、数据架构、技术架构和安全架构。积极协调相关部门共同推动需求整合，在企业架构指导下进行具体系统的实施，并通过架构管控落实信息安全政策、标准和技术实现。

2. 加强信息科技队伍建设，提高自主开发和运维能力

加强银行信息技术条线人员流动，从各中心选拔经验丰富的优秀人才充实管理队伍，新进员工补充到开发一线，形成合理的开发和管理梯队；适度调度分行开发人员参与总行项目的开发工作，优化银行信息技术资源配备。参照国际一流和国内最佳做法，建立信息科技自主开发、自主运维能力模型，量化信息科技自主开发、自主运维评价指标，组织开展信息科技自主开发、自主运维能力评价和考核，引导鼓励员工自主开发、自主运维，确保信息系统核心能力、安全生产运行等关键环节掌握在本行技术人员手中。

3. 定期开展信息科技检查

为了促进信息科技制度落实，规范信息科技合规的检查管理，银行组织制定印发《信息科技工作检查管理办法》和《信息科技工作检查标准》等信息科技检查相关规章制度，明确全行信息科技检查范围、检查对象、检查频率及检查标准，并由总行信息技术管理部领导亲自带队开展现场检查，指导整改，将检查发现问题和经验交流结果通报全行，促进信息科技各项制度的落实，有效防范操作风险。

2.4.6 针对新形势积极探索信息安全应对策略

银行与经济发展密切相关，银行信息系统建设也始终围绕更好地为客户经济活动提供金融服务展开。在“走出去”、客户全球化、交易电子化、服务无界化的大背景下，银行业将面对如何在更开放的环境中提供安全金融服务的挑战；信息技术的迅猛发展，打破了原有的业界信息安全基准，公认的验证完整性的 MD5 算法也已在云计算的背景下被证明存在安全缺陷，云计算的兴起，提供了充足的计算资源，使得暴力破解密码更为轻松，网上唾手可得的攻击工具和有组织的金融犯罪等均对银行信息安全防护提出了严峻挑战；同时，面对错综复杂的金融环境，合理平衡安全与易用的关系，在保障客户资金交易安全的同时兼顾客户便利也是银行业面对的长期挑战。

单纯的防御已显得力不从心，面对挑战，银行业正采取更加积极的态度去面对，跟踪信息技术发展趋势，及时淘汰落后的信息安全技术和产品，更新信息安全技术和安全产品选用策略，完善信息安全技术和安全产品使用指南，提升信息安全防护能力。主要表现在：

1）将安全防线前移，在客户端引入安全扫描等机制，主动评价客户平台安全状况，加强客户平台准入管理，增强客户异常行为检查，通过识别客户交易时段、地点、交易频率及额度等信息，提前预警防范风险；加强纵深防御，在防线前移的同时，增加后台安全管理手段，建立业务安全监控机制，及时识别危险账户和客户异常行为，实现

技术防范与业务交易安全监控联动，更有针对性地防范风险。

2）全面贯彻银监会对等级保护和信息科技风险管理的主旨思想，根据《商业银行信息科技风险管理指引》的要求，按照信息系统承载的价值、一旦失效对客户和社会的影响进行信息系统等级划分，针对不同等级的信息系统采取相应的安全等级保护。同时，应用等级化保护策略，对客户账户类型和客户风险承受能力进行安全等级划分，区别设置验证策略和监控防控手段，更人性化、更安全地提供金融服务。

3）大力改善基础设施。近年来，银行持续推进灾备中心建设，组织制定了信息科技服务连续性建设近、中、远期目标，明确了生产与灾备中心布局策略及总、分行信息系统灾备建设策略，确立了信息系统灾备分级及恢复策略，完成了信息科技系统灾备总体方案，明确了灾备体系实施路径。目前，各商业银行数据中心均符合国家最新 A 类机房建设标准，数据中心运行环境得到了极大改善；银行分布在全国的各家分行机房也在陆续的改造和设备更新中，逐步消除了机房容量不足、设备老化、电力保障薄弱、缺乏双回路等隐患，改善了我国银行信息科技运行环境。

4）开展重要信息系统风险排查和整改优化。各商业银行能够有效落实银监会发布的风险警示，吸取业界信息安全事件经验教训，对信息服务的关键系统进行了全面梳理，组织系统失效点排查、系统高可用性设计分析、服务接口安全风险分析，评析系统故障发生后的业务影响，制定系统优化改进方案，组织系统优化，增强系统可用性。

第二篇

管理篇

本篇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，系统地分析了银行信息安全管理体系包含的相关内容，并给出了信息安全管理体系参考的框架结构。在此基础上，本篇就信息安全管理的各个组成模块进行了详细介绍，包括信息安全方针、信息安全组织及人员安全管理、信息安全管理制度、信息安全风险管理、信息安全规划与建设、信息安全监控与监察、信息安全事件管理与应急响应、信息系统灾难恢复管理及信息安全审计等内容。

第 3 章
银行信息安全管理体系参考框架

信息安全包含的内容相当广泛，以各自独立的视角去看待信息安全就会只见树木不见森林。因此，应将银行信息安全管理当作一个整体加以研究和应用。

信息安全管理体系参考框架就是从整体上去看待银行信息安全的所有工作。由于每家银行都具有各自不同的特点，因此并不存在一个统一的信息安全管理体系适合所有银行。本章提出的信息安全管理体系参考框架，对银行业信息安全管理体系进行了提炼，在框架层面具有普遍性，但是每家银行在进行信息安全管理体系建设时，需要根据自身实际对具体内容进行修改、调整和细化。本章先是介绍了信息安全管理体系的各种参考标准，然后在此基础上根据银行业的特点，对银行业信息安全管理体系参考框架进行了总结和描述。

3.1 信息安全管理体系参考标准和规范

3.1.1 银行业信息科技风险管理指引

2006 年 9 月，为有效防范银行业金融机构运用信息系统进行业务处理、经营管理和内部控制过程中产生的风险，促进我国银行业安全、持续、稳健运行，银监会印发了银监发［2006］第 63 号文，即《银行业金融机构信息系统风险管理指引》。

2009 年 6 月，为加强商业银行信息科技风险管理，根据《中华人民共和国银行业监督管理法》《中华人民共和国商业银行法》《中华人民共和国外资银行管理条例》及国家信息安全相关要求和有关法律法规，银监会印发了银监发［2009］第 19 号文，即《商业银行信息科技风险管理指引》，以替代旧的《银行业金融机构信息系统风险管理指引》。

新《指引》针对银行业信息科技风险特点，提出了“三道防线”的思路。“三道防线”是按照目前普遍的一种安全模式进行的设计：第一道防线——事先监控，即银行

信息科技部门的自我管理；第二道防线——事中管理，即风险管理部门如何督促科技部门进行管理，风险管理部门会提供一些管理工具、思路和框架；第三道防线——事后审计，审计部门独立于上述两个部门之外，对两部门执行情况进行评价。因此三道防线其实是将信息科技管理、信息科技风险管理、信息科技风险审计统一纳入风险管控。通过这样的思想，可以很好地解决银行重建设、轻管理、重开发、轻运维的不足。

《商业银行信息科技风险管理指引》包括了以下内容：

第一章　总则。本章对《商业银行信息科技风险管理指引》进行了总体说明和术语定义。

第二章　信息科技治理。本章对商业银行在信息科技治理方面提出了相应的要求，包括法定代表人、董事会、首席信息官、信息科技风险管理部门、信息科技风险审计等高层人员和相关部门在信息科技风险上的职责和义务。

第三章　信息科技风险管理。本章对商业银行的具体风险管理工作提出了要求，包括信息科技风险管理策略、风险识别和评估流程、风险防范措施、信息科技风险计量和监测机制。

第四章　信息安全。本章对商业银行信息安全工作提出了要求，包括信息分类保护、人员培训、信息安全流程、物理安全、网络安全、系统应用安全、安全日志记录和加密、终端安全等内容。

第五章　信息系统开发、测试和维护。本章对商业银行在信息系统的生命周期安全控制方面提出了要求，包括信息系统需求分析、规划、采购、开发、测试、部署、维护、升级和报废等阶段的要求。

第六章　信息科技运行。本章对商业银行在信息科技日常运行过程中的要求进行了规定。包括物理环境选择、职责分离规定、交易记录保存、信息安全事故管理、性能及容量管理、变更管理等。

第七章　业务连续性管理。本章对商业银行在业务连续性方面的工作提出了要求，包括业务连续性计划、资源提供、演练和培训等。

第八章　外包管理。本章对商业银行在外包管理方面提出了相应要求。

第九章　内部审计和第十章　外部审计。分别对内、外部信息科技审计提出了要求。

第十一章　附则。本章明确了银监会监督检查、解释等职责，对《指引》的施行等内容进行了规定。

在《商业银行信息科技风险管理指引》的第四章，对于信息安全管理进行了相应描述，指出信息安全策略应涉及以下领域：

（一）安全制度管理

（二）信息安全组织管理

（三）资产管理

（四）人员安全管理

（五）物理与环境安全管理

（六）通信与运营管理

（七）访问控制管理
（八）系统开发与维护管理
（九）信息安全事件管理
（十）业务连续性管理
（十一）合规性管理

3.1.2 等级保护

1. 等级保护概述

信息安全等级保护制度是国家信息安全保障工作的基本制度、基本策略和基本方法，是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。国务院法规和中央文件明确规定，要实行信息安全等级保护，重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度。信息安全等级保护是当今发达国家保护关键信息基础设施、保障信息安全的通行做法，也是我国多年来信息安全工作经验的总结。开展信息安全等级保护工作不仅是保障重要信息系统安全的重大措施，也是一项事关国家安全、社会稳定、国家利益的重要任务。

为组织各单位、各部门开展信息安全等级保护工作，公安部根据法律授权，会同国家保密局、国家商用密码管理办公室和原国务院信息办组织开展了基础调查、等级保护试点、信息系统定级备案、安全建设整改等重要工作，出台了一系列政策文件，构成了信息安全等级保护政策体系，为指导各地区、各部门开展等级保护工作提供了政策保障。同时，在国内有关部门、专家、企业的共同努力下，公安部和标准化工作部门组织制定了信息安全等级保护工作需要的一系列标准，形成了信息安全等级保护标准体系，为开展信息安全等级保护工作提供了标准保障。

信息安全等级保护广义上指涉及该工作的标准、产品、系统、信息等均依据等级保护思想的安全工作；狭义上一般指信息系统安全等级保护，是指对国家安全、法人和其他组织及公民的专有信息及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应并处置的综合性工作。

2. 等级保护的等级划分

《信息安全等级保护管理办法》规定，国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度和信息系统遭到破坏后对国家安全、社会秩序、公共利益及公民、法人和其他组织的合法权益的危害程度等因素确定。

信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

3. 信息系统安全保护等级的定级要素

信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。

（1）受侵害的客体 等级保护对象受到破坏时所侵害的客体包括以下 3 个方面：

1）公民、法人和其他组织的合法权益。

2）社会秩序、公共利益。

3）国家安全。

（2）对客体的侵害程度 对客体的侵害程度由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的，因此，对客体的侵害外在表现为对等级保护对象的破坏，通过危害方式、危害后果和危害程度加以描述。等级保护对象受到破坏后对客体造成侵害的程度归结为以下三种：

1）造成一般损害。

2）造成严重损害。

3）造成特别严重损害。

4. 等级保护的一般流程

信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，信息系统定级也应由业务信息安全和系统服务安全两方面确定。

从业务信息安全角度反映的信息系统安全保护等级称为业务信息安全保护等级。从系统服务安全角度反映的信息系统安全保护等级称为系统服务安全保护等级。确定信息系统安全保护等级的一般流程如下：

1）确定作为定级对象的信息系统。

2）确定业务信息安全受到破坏时所侵害的客体。

3）根据不同的受侵害客体，从多个方面综合评定业务信息安全被破坏对客体的侵害程度。

4）得到业务信息安全保护等级。

5）确定系统服务安全受到破坏时所侵害的客体。

6）根据不同的受侵害客体，从多个方面综合评定系统服务安全被破坏对客体的侵害程度。

7）得到系统服务安全保护等级。

8）将业务信息安全保护等级和系统服务安全保护等级的较高者确定为定级对象的安全保护等级。

5. 等级保护的实施原则

根据《信息系统安全等级保护实施指南》，信息系统安全等级保护实施过程中，应坚持以下基本原则：

1）自主保护原则：信息系统运营、使用单位及其主管部门按照国家相关法规和标准，自主确定信息系统的安全保护等级，自行组织实施安全保护。

2）重点保护原则：根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统。

3）同步建设原则：信息系统在新建、改建、扩建时应当同步规划和设计安全方案，投入一定比例的资金建设信息安全设施，保障信息安全与信息化建设相适应。

4）动态调整原则：要跟踪信息系统的变化情况，调整安全保护措施。由于信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级，根据信息系统安全保护等级的调整情况，重新实施安全保护。

6. 等级保护基本要求

信息系统安全等级保护应依据信息系统的安全保护等级情况保证它们具有相应等级的基本安全保护能力，不同安全保护等级的信息系统要求具有不同的安全保护能力。

基本安全要求是针对不同安全保护等级信息系统应该具有的基本安全保护能力提出的安全要求，根据实现方式的不同，基本安全要求分为基本技术要求和基本管理要求两大类。技术类安全要求与信息系统提供的技术安全机制有关，主要通过在信息系统中部署软硬件并正确地配置其安全功能来实现；管理类安全要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程及记录等方面做出规定来实现。

基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面提出；基本管理要求从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个方面提出；基本技术要求和基本管理要求是确保信息系统安全不可分割的两个部分。

基本安全要求从各个层面或方面提出了系统的每个组件应该满足的安全要求，信息系统具有的整体安全保护能力通过不同组件实现基本安全要求来保证。除了保证系统的每个组件满足基本安全要求外，还要考虑组件之间的相互关系，来保证信息系统的整体安全保护能力。

3.1.3 ISO/IEC 27001

ISO/IEC 27001 是针对信息安全管理体系要求的国际标准，其前身为英国的 BS

7799 标准，该标准由英国标准协会（BSI）于 1995 年 2 月提出，并于 1995 年 5 月修订而成。1999 年 BSI 重新修改了该标准。BS 7799 分为两个部分：BS 7799-1，信息安全管理实施规则；BS 7799-2，信息安全管理体系规范。

第一部分对信息安全管理给出建议，供负责在其组织启动、实施或维护安全的人员使用；第二部分说明了建立、实施和文件化信息安全管理体系的要求，规定了根据独立组织的需要应实施安全控制的要求。

BS 7799-1 与 BS 7799-2 经过修订于 1999 年重新发布，1999 版考虑了信息处理技术，尤其是在网络和通信领域应用的近期发展，同时还非常强调了商务涉及的信息安全及信息安全的责任。

2000 年 12 月，BS 7799-1：1999《信息安全管理实施细则》通过了国际标准化组织 ISO 的认可，正式成为国际标准——ISO/IEC 17799：2000《信息技术—信息安全管理实施细则》。2002 年 9 月 5 日，BS 7799-2：2002 草案经过广泛的讨论之后，终于发布成为正式标准，同时 BS 7799-2：1999 被废止。2004 年 9 月 5 日，BS 7799-2：2002 正式发布。2005 年，BS 7799-2：2002 终于被 ISO 组织所采纳，于同年 10 月推出 ISO/IEC 27001：2005。

2005 年 6 月，ISO/IEC 17799：2000 经过改版，形成了新的 ISO/IEC 17799：2005，新版本较老版本无论是组织编排还是内容完整性上都有了很大的增强和提升。ISO/IEC 17799：2005 已更新并在 2007 年 7 月 1 日正式发布为 ISO/IEC 27002：2005，这次更新只是改变了标准号，内容并没有改变。

2013 年 10 月 1 日，国际标准化组织 ISO 发布了 ISO/IEC 27001：2013《信息技术—安全技术—信息安全—管理体系—要求》（Information technology—Security technique—Information security management systems—Requirement）。该标准代替了 ISO/IEC 27001：2005。我国正按照等同采用的原则，由全国信息安全标准化技术委员会（SAC/TC260）负责将 ISO/IEC 27001：2013 转换为国家标准（即新版 GB/T 22080），以代替原 GB/T 22080—2008。2013 年 10 月国际认可论坛（IAF）成员大会，通过了有关 ISO/IEC 27001：2013 转换的决议（编号为：IAF Resolution 2013-13）。该决议规定：

1）符合 ISO/IEC 27001：2013 的截止日为该标准发布之后的 2 年，即转换截止日期为 2015 年 9 月 30 日。

2）自该标准发布一年后（即 2014 年 10 月 1 日），所有新颁发的、获认可的认证证书均应依据 ISO/IEC 27001：2013。

ISO/IEC 27001：2013 标准第 4 ~ 7 章，说明管理体系的一般要求，包括组织的情境、领导力、策划和支持；标准第 8 章，描述信息安全管理体系（Information Security Management System，ISMS）实施要求，包括信息安全风险评估和处置；标准第 9 章，描述监视、测量和评审活动的要求；标准第 10 章，描述改善活动的要求；其中，取消了关于预防措施的内容。新版 ISO/IEC 27001：2013 标准中，信息安全风险管理要求与 ISO 31000：2009《风险管理——原则与实施指南》（Risk management—Principles and guidelines）保持一致，并遵从其中的定义。

在 ISO/IEC 27001：2013 标准中明确了以下要求：

组织应确定如何确定其信息安全风险评估和处置过程的可靠性。适用时，组织应调整信息安全风险评估和处置过程及采用的方法，以改善过程的可靠性。新版 ISO/IEC 27001 依然会保留 SOA 和附录 A 控制目标、控制措施的架构。

（1）安全策略 制定信息安全方针，为信息安全提供管理指引和支持，并定期评审。

（2）信息安全的组织 建立信息安全管理组织体系，在内部开展和控制信息安全的实施。

（3）人力资源安全 确保所有员工、合同方和第三方了解信息安全威胁和相关事宜及各自的责任和义务，以减少人为差错、盗窃、欺诈或误用设施的风险。

（4）资产管理 核查所有信息资产，做好信息分类，确保信息资产受到适当程度的保护。

（5）访问控制 制定访问控制策略，避免信息系统的非授权访问，并让用户了解其职责和义务，包括网络访问控制，操作系统访问控制，应用系统和信息访问控制，监视系统访问和使用，定期检测未授权的活动；当使用移动办公和远程控制时，也要确保信息安全。

（6）密码 确保适当和有效地使用密码，保护信息的保密性、真实性或完整性。

（7）物理和环境安全 定义安全区域，防止对办公场所和信息的未授权访问、破坏和干扰；保护设备的安全，防止信息资产的丢失、损坏或被盗，防止对企业业务的干扰；同时，还要做好一般控制，防止信息和信息处理设施的损坏和被盗。

（8）操作管理 制定操作规程和职责，确保信息处理设施的正确和安全操作；建立系统规划和验收准则，将系统失效的风险降到最低；防范恶意代码和移动代码，保护软件和信息的完整性；做好信息备份和网络安全管理，确保信息在网络中的安全，确保其支持性基础设施得到保护；建立媒体处置和安全的规程，防止资产损坏和业务活动的中断；防止信息和软件在组织之间交换时丢失、修改或误用。

（9）通信安全 通信安全是确保正确、安全地维护组织与任何外部实体的信息传输安全，确保网络和其支持信息处理设施中信息的保护。

（10）系统采集、开发和维护 标示系统的安全要求，确保安全成为信息系统的内置部分，控制应用系统的安全，防止应用系统中用户数据的丢失、修改或误用；通过加密手段保护信息的保密性、真实性和完整性；控制对系统文件的访问，确保系统文档、源程序代码的安全；严格控制开发和支持过程，维护应用系统软件和信息安全。

（11）供方关系 确保保护供方访问的组织资产的安全，根据供应商协议，维护信息安全和服务交付的商定水平。

（12）信息安全事件管理 报告信息安全事件和弱点，及时采取纠正措施，确保使用持续有效的方法管理信息安全事件，并确保及时修复。

（13）业务连续性管理 目的是减少业务活动的中断，使关键业务过程免受主要故障或天灾的影响，并确保及时恢复。

（14）符合性 信息系统的设计、操作、使用过程和管理要符合法律法规的要求，符合组织安全方针和标准，还要控制系统审计，使信息审核过程的效力最大化，干扰最小化。

除了 ISO/IEC 27001，ISO/IEC 27000 包括一系列标准：

ISO/IEC 27000 信息安全管理体系—概述与术语（ISMS Overview and vocabulary）

ISO/IEC 27001 信息安全管理体系—要求（ISMS Requirements）（以 BS 7799-2 为基础）

ISO/IEC 27002 信息安全管理实践规范（Code of practice for inform ation security manage ment）（ISO/IEC 17799：2005）

ISO/IEC 27003 信息安全管理体系—实施指南（ISMS Implementation guidance）

ISO/IEC 27004 信息安全—测量（Information security—Measurement）

ISO/IEC 27005 信息安全风险管理（Information security risk management）

ISO/IEC 27006 信息安全管理体系—认证机构的认可要求（Requirements for bodies providing audit and certification of information security management systems）

ISO/IEC 27007 信息安全管理体系审核员指南（Guidelines for information security management systems auditing）

3.1.4 COSO

COSO 是美国反虚假财务报告委员会下属的发起人委员会（The Committee of Sponsoring Organizations of the Treadway Commission）的英文缩写。1985 年，由美国注册会计师协会、美国会计协会、财务经理人协会、内部审计师协会、管理会计师协会联合创建了反虚假财务报告委员会，旨在探讨财务报告中的共谋产生的原因，并寻找解决之道。两年后，基于该委员会的建议，其赞助机构成立 COSO 委员会，专门研究内部控制问题。1992 年 9 月，COSO 委员会发布《内部控制整合框架》，简称 COSO 报告，1994 年进行了增补。

COSO 委员会从 2001 年起开始进行企业风险管理方面的研究，在 2003 年 7 月完成了《企业风险管理框架（草案）》并公开向业界征求意见。2004 年 4 月美国 COSO 委员会在《内部控制整体框架》的基础上，结合《萨班斯—奥克斯法案》（Sarbanes—Oxley Act）在报告方面的要求，同时吸收各方面风险管理研究成果，颁布了《企业风险管理框架》（Enterprise Risk Management Framework），旨在为各国的企业风险管理提供一个统一术语与概念体系的全面的应用指南。

COSO 和《企业风险管理框架》的基本内容包括：

1. 控制环境（control environment）

它包括组织人员的诚实、伦理价值和能力；管理层哲学和经营模式；管理层分配权限和责任、组织、发展员工的方式；董事会提供的关注和方向。控制环境影响员工的管理意识，是其他部分的基础。

2. 风险评估（risk assessment）

风险评估是确认和分析实现目标过程中的相关风险，是形成管理何种风险的依据。它随经济、行业、监管和经营条件而不断变化，需建立一套机制来辨认和处理相应的风险。

3. 控制活动（control activities）

控制活动是帮助执行管理指令的政策和程序。它贯穿整个组织、各种层次和功能，包括各种活动，如批准、授权、证实、调整、经营绩效评价、资产保护和职责分离等。

4. 信息的沟通与交流（information and communication）

信息系统产生各种报告，包括经营、财务、合规等方面，使得对经营的控制成为可能。处理的信息包括内部生成的数据，也包括可用于经营决策的外部事件、活动、状况的信息和外部报告。所有人员都要理解自己在控制系统中所处的位置及相互的关系；必须认真对待控制赋予自己的责任，同时也必须同外部团体如客户、供货商、监管机构和股东进行有效的沟通。

5. 对环境的监控（monitoring）

监控在经营过程中进行，通过对正常的管理和控制活动及员工执行职责过程中的活动进行监控，来评价系统运作的质量。不同评价的范围和步骤取决于风险的评估和执行中的监控程序的有效性。对于内部控制的缺陷要及时向上级报告，严重的问题要报告到管理层高层和董事会。

COSO 是企业内部控制和风险管理的框架，而 COSO 委员会在信息技术治理指南中将信息技术安全架构界定为内部控制和风险防范的起点与核心，说明信息技术治理需要重点关注信息安全的识别和防范。而银行需要建立完善、健全的信息安全架构来规范信息技术治理行为，通过建立风险控制机制来降低银行的信息技术风险。

3.1.5 COBIT

信息及相关技术的控制目标（Control Objectives for Information and Related Technology，COBIT）是目前国际上通用的信息系统治理和管理的标准，由信息系统审计与控制协会（ISACA）在 1996 年公布。这是一个在国际上公认的、权威的安全与信息技术管理和控制的标准，目前已经更新至 5.0 版。它在商业风险、控制需要和技术问题之间架起了一座桥梁，以满足管理的多方面需要。该标准体系已在世界上一百多个国家的重要组织与企业中运用，指导这些组织有效利用信息资源，有效地管理与信息相关的风险。

1. 通过实施 COBIT 可带来的收益

COBIT 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，如对最终成果的评价、对建设过程的评价、对系统架构的评价等。COBIT 是一个基于信息技术治理概念的、面向信息技术建设过程的信息技术

治理实现指南和审计标准。

COBIT是一个非常有用的工具，也非常易于理解和实施，可以帮助企业在管理层、信息技术与审计之间交流的鸿沟上搭建桥梁，提供了彼此沟通的共同语言。几乎每个机构都可以从COBIT中获益，来决定基于信息技术过程及他们所支持的商业功能的合理控制。当我们知道这些业务功能是什么，其对企业的影响到什么程度时，就能对这些事件进行良好的分类。

通过实施COBIT，增加了管理层对控制的感知及支持。COBIT帮助管理层懂得如何控制影响和业务功能。COBIT提供的实施工具集包括优秀的案例资料（提供模板业务过程，使得优秀范例能够迅速移植），有助于向管理层很好地表述信息技术管理概念。管理层基于最佳控制实践做出正确决策的能力亦得到了提高。

COBIT使信息技术管理工作简易并量化，降低复杂信息系统管理工作的难度。对于那些不具有广博信息技术知识的人来讲，是一个认清信息技术的有价值的工具。它也使得信息系统审计师具有与信息技术专业人员相同的专业广度，并且可以询问信息技术工程相关的问题。

COBIT提供了一种国际通用的信息技术管理及问题解决方案，普遍适用于各种不同的业务项目和审计，并且既包容了当前的情况，也提供将来可能会使用到的指导方针。

COBIT有助于提高信息系统审计师的影响力，依据COBIT出具的信息系统审计报告，更容易得到管理层的肯定。

COBIT框架能够帮助决定过程责任，提高信息技术治理水平。通过应用该框架进行责任分析，可以做到基于角色的信息技术管理，定义过程措施，确保客户利益。

2. COBIT有过的五个主要版本

1）1996年，第一版推出。

2）1998年，第二版推出，包括了“管理指南”。

3）2000年，第三版推出。2003年，此版本可以从网上获得。

4）2005年12月，第四版首次推出。2007年5月，发行其修订版COBIT 4.1。

5）2012年6月，COBIT 5.0发行。它巩固并集合了COBIT 4.1、Val IT 2.0和RISK信息技术框架，同时从BMIS和ITAF中汲取了部分内容。

COBIT 5.0为企业信息技术治理和管理提供的新一代指引，是以来自商务、信息技术、风险、安全和鉴证团体的众多企业和用户对COBIT超过15年的实际使用和应用为依据而构建的。COBIT 5.0提供了一种全面的框架，以支持企业实现其企业信息技术治理和管理的目标。简而言之，就是帮助企业通过维持实现利益、优化风险等级及资源利用之间的平衡，从而创造源自于信息技术的最佳价值。COBIT 5.0能够为整个企业使信息技术在整体上得以治理和管理，并承担整个端到端业务和信息技术功能区域的责任，同时兼顾内外部利益相关者与信息技术相关的利益。COBIT 5.0可用于各种规模的机构，包括商务、非营利或公共机构。

COBIT 5.0提出了能使组织在一套包含7个驱动因素的整体方法下建立有效治理和管理框架的5个原则，以优化信息和技术的投资及使用以满足利益相关者的利益。

3. COBIT 的 5 个原则

1）满足利益相关者的需求。

2）覆盖组织的端到端。

3）应用一个单一的整合性框架。

4）运用了整体方法。

5）将治理从管理中分离。

4. COBIT 的 7 个驱动因素

1）原则、策略和框架是将期望的行为转化为实际指南的手段，以便于日常管理。

2）程序描述了一系列有组织的实践和活动以实现既定的目标，同时产生一系列结果以支持实现全部信息技术相关的目标。

3）组织架构是企业中决策的关键实体。

4）个人和企业的文化、道德和行为作为治理和管理活动的成功因素经常被忽略。

5）信息是保持组织运营和良好治理所必需的，但在操作层面，信息往往是企业本身的关键产品。

6）服务、基础架构和应用系统包括为组织提供信息技术处理和服务的基础架构、技术及应用系统。

7）人员、技能和能力是成功完成所有活动，并做出正确选择及采取纠正措施所必需的部分。

总之，COBIT 模型实现了企业战略与信息技术战略的互动，并形成持续改进的良性循环机制，为企业提供了具有一定参考价值的解决方案。因此，针对我国信息化存在的问题，借鉴 COBIT 的信息技术治理思想和框架，科学、系统地对信息及相关技术进行管理，逐步试行建立信息技术治理机制，对推动我国信息技术的发展和应用具有十分重要的现实意义。

COBIT 通过支持业务目标所需信息，以及被信息技术流程管理的、由信息技术相关的应用工具所产生的信息，来实现对信息和信息技术的控制。由于信息必须是安全的才会对业务目标有用，所以对于信息安全的要求是 COBIT 的内在要求。

3.1.6 ITIL

信息技术基础架构库（Information Technology Infrastructure Library，ITIL）由英国政府部门中央计算和电信局（Central Computing and Telecommunications Agency，CCTA）在 20 世纪 80 年代末制定，现由英国商务部（Office of Government Commerce，OGC）负责管理，主要适用于信息技术服务管理（ITSM）。ITIL 为企业的信息技术服务管理实践提供了一个客观、严谨、可量化的标准和规范。

自提出 ITIL 以来，ITIL 作为信息技术服务管理事实意义上的国际标准已经得到了全球几乎所有信息技术巨头的全力支持。IBM、惠普、微软、CA、BMC、ASG 等著名

跨国公司作为 ITIL 的积极倡导者，基于 ITIL 分别推出了实施信息技术服务管理的软件和实施方案。ITIL 在欧洲、北美洲、大洋洲已得到广泛应用，全球 1 万多家在各行业处于领先地位的著名企业给我们带来了众多实施 ITIL 的成功案例，通过实施 ITIL 大大改进了企业信息技术服务的质量，促进了信息技术与业务的融合。

企业的信息技术部门和最终用户可以根据自己的能力和需求定义自己所要求的不同服务水平，参考 ITIL 来规划和制定其信息技术基础架构及服务管理，从而确保信息技术服务管理能为企业的业务运作提供更好的支持。对企业来说，实施 ITIL 的最大意义在于把信息技术与业务紧密地结合起来了，从而让企业的信息技术投资回报最大化。

自从 1980 年至今，ITIL 经历了三个主要的版本：

1）Version 1——1986—1999 年原始版，主要是基于职能型的实践，开发了 40 多卷图书。

2）Version 2——1999—2006 年 ITIL v2 版，主要是基于流程型的实践，共有 10 本图书，包含 7 个体系：服务支持、服务提供、实施服务管理规划、应用管理、安全管理、基础架构管理及 ITIL 的业务前景。它已经成为信息技术服务管理领域全球广泛认可的最佳实践框架。

3）Version 3——2004—2007 年基于服务生命周期的 ITIL v3 整合了 v1 和 v2 的精华，并与时俱进地融入了信息技术服务管理领域当前的最佳实践。5 本生命周期图书形成了 ITIL v3 的核心，它主要强调 ITIL 最佳实践的执行支持和在改善过程中需要注意的细节。

ITIL 最新版本是 v3.0，于 2011 年发布，包含信息技术的 5 个生命周期：战略阶段（Service Strategy）、设计阶段（Service Design）、转换阶段（Service Transition）、运营阶段（Service Operation）、改进阶段（Service Improvement）。

每一个生命周期对应了相应的指导文件：

1）服务战略指导文件提供了基于市场驱动模型的信息技术服务方法。它描述了一系列的管理流程，可以帮助企业根据财务效益原则做出更精准的外包决策。

2）服务设计指导文件解释了信息技术服务对较大的业务怎样产生影响。它涵盖了信息技术服务的设计实例和技术服务的交付、服务管理工具、ITIL 服务支持流程、支撑服务的供应链。具体的管理业务内容包括服务水平、可用性、容量和安全管理。

3）服务转换指导文件讲解了将业务需求转化为实际信息技术服务的过程。ITIL 服务管理约定你必须以项目管理的模式完成这些转换过程，同时，服务转换指导文件也说明了应该如何完成业务环境下的变更管理。服务转换包括变更管理、资产和配置管理、软件发布或部署管理、服务测试等。

4）服务运营指导文件提供了一系列范例，帮助企业向其员工、合作伙伴和客户交付所需的服务水平——这也是信息技术在整个 ITIL 生命周期中真正创造价值的部分。ITIL 服务从业人员接受的培训包括如何处理日常事务和事故、回应请求、管理问题、维护安全性。

5）服务的持续改进指导文件协助企业确定需要服务变更的节点，配合业务需求的变化持续调整服务，同时掌控全局，考核变更的成效。这涉及考核节点的定义和考核数

据的收集、处理和分析。当需要改进时，信息技术团队会执行变更流程，通过前面的考核数据评估成效，并依此推广到更多标准化的变更。这是一个持续的过程。

虽然 ITIL v3. 0 不是从流程的角度对信息技术管理进行描述，但其本质和核心仍然是各种流程，下面对这些流程进行简要的介绍。

1）服务台：服务台是信息技术部门和信息技术服务用户之间的单一联系点。它通过提供一个集中和专职的服务联系点促进了组织业务流程与服务管理基础架构集成。服务台的主要目标是协调客户（用户）和信息技术部门之间的联系，为信息技术服务运作提供支持，从而提高客户的满意度。

2）事件管理：事件管理负责记录、归类和安排专家处理事故并监督整个处理过程直至事故得到解决和终止。事件管理的目的是在尽可能最小地影响客户和用户业务的情况下使信息技术系统恢复到服务级别协议所定义的服务级别。

3）问题管理：问题管理是指通过调查和分析信息技术基础架构的薄弱环节、查明事故产生的潜在原因，并制定解决事故的方案和防止事故再次发生的措施，将由问题和事故对业务产生的负面影响减小到最低的服务管理流程。与事件管理强调事故恢复的速度不同，问题管理强调的是找出事故产生的根源，从而制定恰当的解决方案或防止其再次发生的预防措施。

4）配置管理：配置管理是识别和确认系统的配置项，记录和报告配置项状态和变更请求，检验配置项的正确性和完整性等活动构成的过程，其目的是提供信息技术基础架构的逻辑模型，支持其他服务管理流程，特别是变更管理和发布管理的运作。

5）变更管理：变更管理是指为了在最短的中断时间内完成基础架构或服务的任一方面的变更而对其进行控制的服务管理流程。变更管理的目标是确保在变更实施过程中使用标准的方法和步骤，尽快地实施变更，以将由变更所导致的业务中断对业务的影响减小到最低。

6）发布管理：发布管理是指对经过测试后导入实际应用的新增或修改后的配置项进行分发和宣传的管理流程。发布管理以前又称为软件控制与分发，它由变更管理流程控制。

7）服务级别管理：服务级别管理是为签订服务级别协议（SLAs）而进行的计划、草拟、协商、监控和报告及签订服务级别协议后对服务绩效的评价等一系列活动所组成的一个服务管理流程。服务级别管理旨在确保组织所需的信息技术服务质量在成本合理的范围内得以维持并逐渐提高。

8）信息技术服务财务管理：信息技术服务财务管理是负责预算和核算信息技术服务提供方提供信息技术服务所需的成本，并向客户收取相应服务费用的管理流程，它包括信息技术投资预算、信息技术服务成本核算和服务计费 3 个子流程，其目标是通过量化服务成本减少成本超支的风险、减少不必要的浪费、合理引导客户的行为，从而最终保证所提供的信息技术服务符合成本效益的原则。信息技术服务财务管理流程产生的预算和核算信息可以为服务级别管理、能力管理、信息技术服务持续性管理和变更管理等管理流程提供决策依据。

9）信息技术服务持续性管理：信息技术服务持续性管理是指确保发生灾难后有足够的技术、财务和管理资源来确保信息技术服务持续性的管理流程。信息技术服务持续性管理关注的焦点是在发生服务故障后仍然能够提供预定级别的信息技术服务，从而支持组织的业务持续运作的能力。

10）能力管理：能力管理是指在成本和业务需求的双重约束下，通过配置合理的服务能力使组织的信息技术资源发挥最大效能的服务管理流程。能力管理流程包括业务能力管理、服务能力管理和资源能力管理3个子流程。

11）可用性管理：可用性管理是通过分析用户和业务方的可用性需求并据以优化和设计信息技术基础架构的可用性，从而确保以合理的成本满足不断增长的可用性需求的管理流程。可用性管理是一个前瞻性的管理流程，它通过对业务和用户可用性需求的定位，使得信息技术服务的设计建立在真实需求的基础上，从而避免信息技术服务运作中采用过度的可用性级别，节约了信息技术服务的运作成本。

信息安全风险是企业风险的一部分，因此ISO 31000对于银行信息安全具有很好的指导作用。

3.1.7 ISO 31000

所有类型和规模的组织都面临内部和外部的、使组织不能确定是否及何时实现其目标的因素和影响。这种不确定性所具有的对组织目标的影响就是风险。组织的所有活动都涉及风险。组织通过识别、分析和评定是否运用风险处理修正风险以满足它们的风险准则，来管理风险。通过这个过程，它们与利益相关方进行沟通和协商，监测和评审风险，并为确保不再进一步需求风险处理而修正风险的控制措施。ISO 31000详细描述了这一系统的过程。

尽管所有的组织在某种程度上都在管理风险，但ISO 31000建立了一些为使风险管理变得有效而需要满足的原则。ISO 31000建议，组织制定、实施和持续改进一个框架，其目的是将风险管理过程整合到组织的整体治理、战略和规划、管理、报告过程、方针、价值观和文化中。

风险管理可以在组织多个领域和层次、任何时间，应用到整个组织及具体职能、项目和活动中。

ISO 31000中所描述的通用方法提供了在任何范围和状况下，以系统、清晰、可靠的方式管理风险的原则和指南。在一个综合框架内采用一致性过程有助于确保在组织内有效、有效率和结合性地管理风险。

每一个具体行业或风险管理的应用都产生了各自的需求、受众、观念和准则。因此，ISO 31000的主要特点是将所包含的“确定状况”作为通用风险管理过程开始的活动。“确定状况”将捕获组织的目标，组织所追求目标的环境，组织的利益相关方和风险准则的多样性，所有这些都将帮助揭示和评价风险的性质和复杂性。

ISO 31000描述了风险管理原则、框架、过程之间的关系，如图3-1所示。

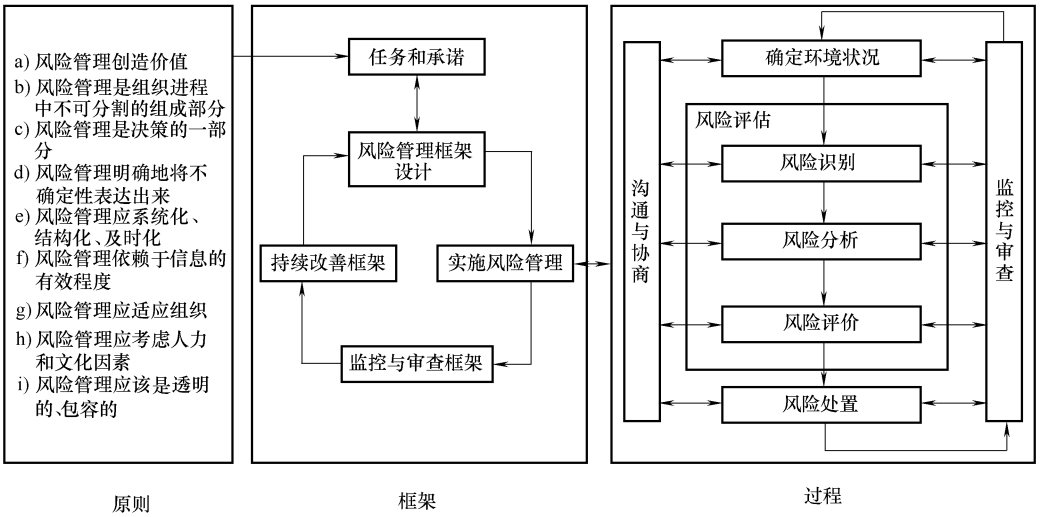


图 3-1　风险管理原则、框架、过程之间的关系

当依据 ISO 31000 实施和保持风险管理时，能够使组织：

1）提高实现目标的可能性。

2）鼓励主动性管理。

3）在整个组织意识到识别和处理风险的需求。

4）改进机会和威胁的识别能力。

5）符合相关法律法规要求和国际规范。

6）改进强制性和自愿性报告。

7）改善治理。

8）提高利益相关方的信心和信任。

9）为决策和规划建立可靠的根基。

10）加强控制。

11）有效地分配和利用风险处理的资源。

12）提高运营的效果和效率。

13）增强健康安全绩效和环境保护。

14）改善损失预防和事件管理。

15）减少损失。

16）提高组织的学习能力。

17）提高组织的应变能力。

ISO 31000 旨在满足众多利益相关方的需求，包括：

1）负责制定组织风险管理方针的人员。

2）负责确保在组织整体、某一特定区域或项目、活动内有效开展风险管理的人员。

3）需要评定组织风险管理有效性的人员。

4）整体或部分地实施风险管理的标准、指南、程序和操作规范的开发者。

目前许多组织的管理实践和过程包含了风险管理的要素，许多组织针对特定类型的风险已经采用了正式的风险管理过程。在这种情况下，组织可以决定对照 ISO 31000 对其现有的实践和过程开展严格的评审。

从巴塞尔协议对操作风险的定义可以看出，操作风险与信息安全具有很大的重合度，但彼此的出发点不一样。操作风险是站在银行风险的角度，而传统信息安全多是站在信息技术的角度。银行进行风险管理时，需要满足巴塞尔协议的要求，因此银行在进行信息安全建设时，也需要参考巴塞尔协议在操作风险上的要求。

3.1.8 《巴塞尔协议》及其操作风险

《巴塞尔协议》的出台源于前联邦德国赫斯塔特（Herstatt）银行和美国富兰克林国民银行（Franklin National Bank）的倒闭。这是两家著名的国际性银行。它们的倒闭使监管机构在惊愕之余开始全面审视拥有广泛国际业务的银行监管问题。赫斯塔特银行和富兰克林国民银行倒闭的第二年，即 1975 年 9 月，第一个《巴塞尔协议》出台。这个协议极为简单，核心内容就是针对国际性银行监管主体缺位的现实，突出强调了两点：①任何银行的国外机构都不能逃避监管；②母国和东道国应共同承担的职责。1983 年 5 月，修改后的《巴塞尔协议》推出。这个协议基本上是前一个协议的具体化和明细化。比如明确了母国和东道国的监管责任和监督权力，分行、子行和合资银行的清偿能力、流动性、外汇活动及其头寸各由哪方负责等，由此体现“监督必须充分”的监管原则。两个《巴塞尔协议》因此也就没有实质性差异：总体思路都是“股权原则为主，市场原则为辅；母国综合监督为主，东道国个别监督为辅”。但是两者对清偿能力等监管内容都只提出了抽象的监管原则和职责分配，未能提出具体可行的监管标准。各国对国际银行业的监管都是各自为战、自成体系，充分监管的原则也就无从体现。

《巴塞尔协议》的实质性进步体现在 1988 年 7 月通过的《关于统一国际银行的资本计算和资本标准的报告》（简称《巴塞尔报告》）。该报告主要有 4 部分内容：①资本的分类；②风险权重的计算标准；③1992 年资本与资产的标准比例和过渡期的实施安排；④各国监管当局自由决定的范围。体现协议核心思想的是前两项。首先是资本的分类，也就是将银行的资本划分为核心资本和附属资本两类，对各类资本按照各自不同的特点进行明确的界定。其次是风险权重的计算标准，报告根据资产类别、性质及债务主体的不同，将银行资产负债表的表内和表外项目划分为 0%、20%、50% 和 100% 4 个风险档次。风险权重划分的目的是为了衡量资本标准服务。有了风险权重，报告所确定的资本对风险资产 8%（其中核心资本对风险资产的比重不低于 4%）的标准目标比率才具有实实在在的意义。可见，《巴塞尔报告》的核心内容是资本的分类。也正因为如此，许多人直接就将《巴塞尔报告》称为规定资本充足率的报告。

2004 年巴塞尔委员会颁布的新资本协议中指出，操作风险是商业银行所面临的另

一种重要风险类型，提出要将信用风险和市场风险之外的操作风险纳入商业银行全面风险管理体系，对操作风险计提风险资本。新资本协议中指出，操作风险指“由不完善或者有问题的内部程序、人员及系统或外部事件所造成损失的风险”。策略风险和声誉风险不包含在此定义中，中国银监会也沿用了该定义。

操作风险经济资本是指，未来一定期间内，在一定的置信水平下，银行为弥补操作风险非预期损失而需要的资本。对操作风险进行计量具有多方面的重要意义。一是监管机构通过计量监管资本，要求金融机构必须持有足够的资本来应对操作风险的非预期损失，从而增强金融机构和金融系统的稳定性；二是金融机构为降低操作风险的资本要求，不断改进管理，从而达到以资本约束扩张、以资本促进管理提升的目的。

3.2 银行实际信息安全管理体系参考框架介绍

3.2.1 银行信息安全管理体系参考框架设计意义

随着我国金融改革的进行，各银行纷纷将竞争的焦点集中到服务手段上，不断加大信息化建设投入，扩大计算机网络规模和应用范围成为一种趋势，信息化在给银行带来利益的同时，也给银行带来了新的安全问题。由于银行信息网络中处理、传输、存储的都是金融信息，对其进行攻击将获得巨额利益。同时，对银行信息网络的攻击，可能对国家安全、社会经济造成重大损失。因此无论从银行信息网络的受关注程度，还是银行信息网络的重要性的角度，都导致银行信息网络的安全问题显得非常重要。

在历经了网络建设、数据大集中、网络安全基础设施建设等阶段后，我国金融信息化已进入了体系化信息安全管理的阶段，通过建立完整的银行信息安全保障体系，有效地防范和化解安全风险，统一安全问题处理规范和流程，增强金融系统的信息安全整体防范能力，以保证金融机构的信息系统平稳运行及各项业务的持续展开。

信息安全管理体系（Information Security Management System，ISMS）作为整个管理体系的一部分，基于业务风险方法，来建立、实施、运行、监审、保持和改进信息安全的体系。ISMS 可以认为是一系列关于组织的信息安全管理的控制措施的总称。

信息安全管理体系为建立、实施、运行、监视、评审、保持和改进 ISMS 提供模型。该标准采用了 PDCA 循环模型，该模型可应用于所有的 ISMS 过程。通过 ISMS 把相关方的信息安全要求和期望作为输入，并通过必要的行动和过程，产生满足这些要求和期望的信息安全结果。

银行信息安全管理体系的意义在于针对银行各信息系统中存在的信息安全风险，从银行的业务需求出发，遵从风险管理的理念，在银行信息技术战略规划的基础上，借鉴国际最佳实践经验，全面指导银行的信息安全工作，并实现以下建设目标：

1）保障业务持续，促进业务发展。

2）保证信息的机密性、完整性和可用性。

3）保证信息的真实性、可核查性、不可否认性和可靠性等特性。

3.2.2 银行信息安全管理体系参考框架设计方法论

信息安全管理体系设计需要以银行信息安全监管要求及实践为基础，参考业界成熟的信息安全管理体系实施方法论，同时结合安全体系评估结果和持续改进方法，最终形成适合特定银行的信息安全管理体系（图3-2）。

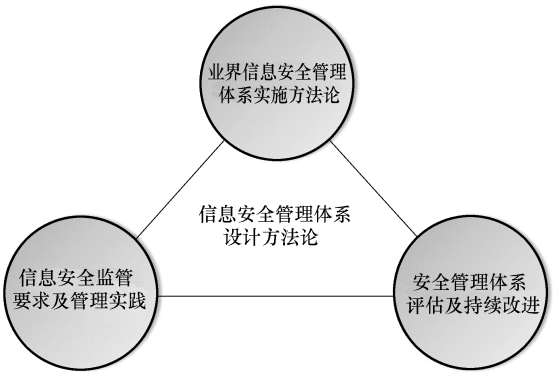


图3-2 典型的信息安全管理体系设计方法论

3.2.3 银行信息安全管理体系参考框架

信息安全包含的内容相当广泛，以各自独立的视角去看待信息安全就会只见树木不见森林。因此，应将银行信息安全管理当作一个整体加以研究和应用。信息安全管理体系参考框架就是从整体上去看待银行信息安全的所有工作。由于每家银行都具有各自不同的特点，因此并不存在一个统一的信息安全管理体系模型适合所有的银行。这里提出的信息安全管理体系模型作为一个参考框架，具有普遍适用性，但是每家银行在进行信息安全管理体系建设时，根据自身实际的不同会有不同的模型。

银行信息安全管理体系参考框架包括以下几个领域：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。银行安全管理体系参考框架如图3-3所示。

1. 信息安全驱动

银行的业务目标、风险策略、审计要求、监管与合规要求、信息科技战略等作为整个组织运作需要考虑的重要因素，同时也对整个信息安全起到驱动作用。银行的信息安全贯穿了信息技术战略和信息技术规划的整个过程。在分解信息化总体架构要求，对各信息系统建设项目的目标、内容、方案和策略等逐一进行规划设计的同时，应该兼顾信

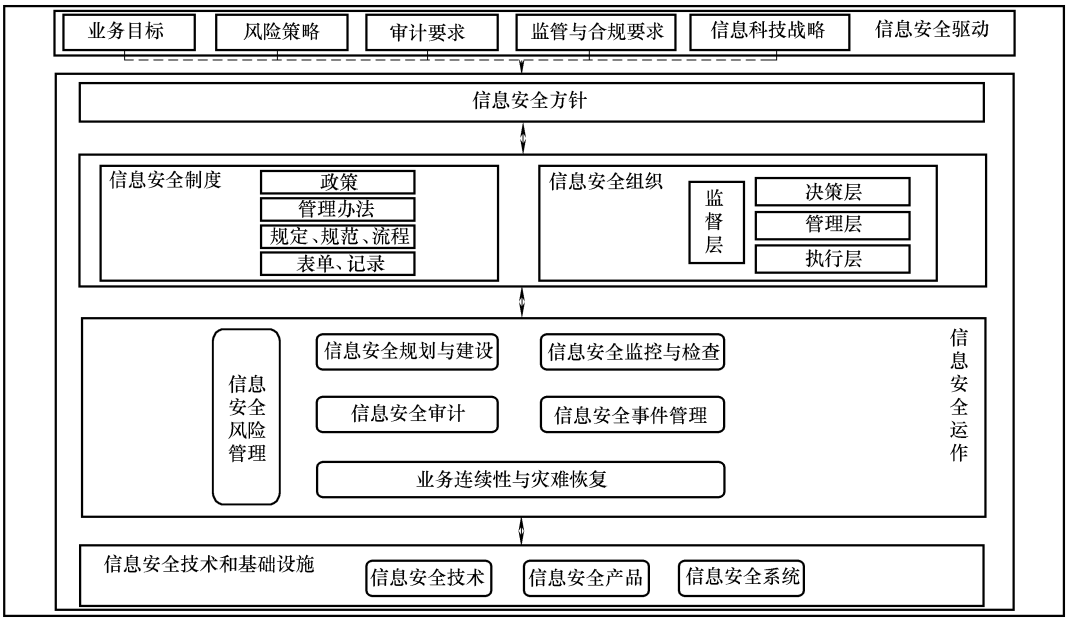


图 3-3　银行安全管理体系参考框架

息安全的规划和建设。

2. 信息安全方针

银行的信息安全方针是为了加强银行信息安全保障能力，建立健全银行的安全管理体系，提高整体的网络与信息安全水平，保证网络通信畅通和业务系统的正常运营，提高网络服务质量，指导银行整体信息安全的工作而制定的信息安全整体策略。

3. 信息安全组织

在明确了安全方针并获得高层管理者的认可后，安全管理的下一步工作就是定义、建立和维护安全组织架构。银行的安全组织架构定义的重要工作之一是定义评估标准，辅助安全管理人员跟踪工作执行情况。首先要定义关键绩效指标（KPI），而后对指标进行长期的维护和修改。

银行信息安全组织通常采用统一领导、分级管理、分级负责的原则。根据银行现有组织结构和运行模式，选择和开发适合的安全组织架构。

安全组织架构解决的具体问题和主要功能如下：

1）明确关键安全功能。

2）明确当前安全职位的人员组成。

3）定义安全管理领导人员的职责。

4）定义安全组织架构和功能。

5）定义安全组织架构的各个角色和职责。

6）定义在企业内的安全部署。

7）定义安全策略、流程和指导原则。

8）定义安全组织架构。

9）管理和检查日常安全操作。

10）与其他业务单元协调。

11）向高层领导汇报。

在银行中，安全应该有专人来总体负责，从建立、实施到维护，全程负责信息的安全工程，并向高层领导汇报。

要求各安全岗位工作人员必须具备较高的道德素质和与岗位相适应的业务技术能力。建立安全技术培训计划，通过各种培训方式，提高各级管理人员和专业人员安全技能，降低安全操作风险。

4. 信息安全制度

银行信息安全制度包括信息安全方针、管理办法、规定、规范、流程、细则、模板表单、记录文件等涉及信息安全的文件。信息安全制度是所有与安全相关活动的基础，其作用是在银行范围内实现安全技术和安全运维的一致性，从而减少安全事件发生的概率、产生的影响和造成的损失。银行的安全制度一经确立，将为安全框架的其他环节提供决策依据。

银行的信息安全方针是信息安全管理的最上层文件，也是信息安全的纲领性文件，其他文件如管理办法、流程、操作规范、技术标准等，都必须遵从这些纲领性文件。

管理办法是信息安全管理制度的约束性文件，是对信息安全某一方面的原则性的规定。

安全管理规定和细则是对管理办法的细化规定和要求。安全规范是实现管理办法需要遵守的准则和规定。包括技术规范和管理规范。安全流程是对管理办法的过程描述，侧重工作过程中输入、输出、活动、职责的界定。

模板表单和记录文件是上述文档制度在执行过程中使用到的相关表单和记录。

5. 信息安全运作

随着信息安全管理体系和技术体系在银行信息安全建设中不断推进，占信息系统生命周期70%～80%的信息安全运作已经越来越被广大从业人员重视。尤其是随着信息系统建设工作从大规模建设阶段逐步转型到“建设和运维”并举的发展阶段，运维人员需要管理越来越庞大的信息技术系统，在这样的情况下，信息安全运作已经被提到了一个空前的高度上。

通常信息安全运作包含两层含义：

1）是指在运维过程中对网络或系统发生病毒或黑客攻击等安全事件进行定位、防护、排除等运维动作，保障系统不受内、外界侵害。

2）对运维过程中发生的基础环境、网络、安全、主机、中间件、数据库乃至核心应用系统发生的影响其正常运行的安全事件，以及围绕安全事件、运维人员和信息资产，依据具体流程而展开监控、告警、响应、评估等运行维护活动。

信息安全运作是一个广泛的概念，从具体内容来看，包括信息安全风险管理、信息

安全规划与建设、信息安全监控与检查、信息安全事件管理、业务连续性与灾难恢复管理及信息安全审计。本书将在后续章节详细阐述各部分内容。

6. 信息安全技术

信息安全的内涵在不断地延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。银行常见的信息安全技术包括：

1）身份认证技术：用来确定用户或者设备身份的合法性，典型的手段有用户名口令、动态口令、PKI 证书和生物认证等。

2）加解密技术：在传输过程或存储过程中进行信息数据的加解密，典型的加密体制可采用对称加密和非对称加密。

3）边界防护技术：防止外部网络用户以非法手段进入内部网络、访问内部资源、保护内部网络操作环境的特殊网络互联设备，典型的设备有防火墙和入侵检测设备。

4）访问控制技术：保证网络资源不被非法使用和访问。访问控制是网络安全防范和保护的主要核心策略，规定了主体对客体访问的限制，并在身份识别的基础上，根据身份对提出资源访问的请求加以权限控制。

5）主机加固技术：操作系统或者数据库的实现会不可避免地出现某些漏洞，从而使信息网络系统遭受严重的威胁。主机加固技术对操作系统、数据库等进行漏洞加固和保护，提高系统的抗攻击能力。

6）安全审计技术：包含日志审计和行为审计，通过日志审计协助管理员在受到攻击后察看网络日志，从而评估网络配置的合理性、安全策略的有效性，追溯分析安全攻击轨迹，并能为实时防御提供手段。通过对员工或用户的网络行为审计，确认行为的合规性，确保管理的安全。

7）检测监控技术：对信息网络中的流量或应用内容进行 OSI（开放式系统互联参考模型）2 ~7 层的检测并适度监管和控制，避免网络流量的滥用、垃圾信息和有害信息的传播。

本书第三篇对信息安全技术进行了详细的介绍，更为细致的内容请参考该篇。

第 4 章
信息安全方针

信息安全工作是银行运营与发展的基础和核心，是保证网络品质的基础，是保障客户利益的基础。信息安全方针是信息安全工作的高度浓缩、提炼和整体指导策略，为了加强银行信息安全保障能力，建立健全银行的安全管理体系，需要建立信息安全方针并根据方针指导实际工作。本章介绍了信息安全方针的基本概念、原则和主要内容。

4.1 信息安全方针概述

信息安全方针是为了加强银行信息安全保障能力，建立健全的银行安全管理体系，提高整体的网络与信息安全水平，保证网络通信畅通和业务系统的正常运营，提高网络服务质量，指导银行整体信息安全的工作而制定的信息安全整体策略。

信息安全方针需要明确信息安全是银行各部门所有员工共同分担的责任，与每一个员工的日常工作息息相关，所有员工必须提高认识，高度重视，从自己开始，坚持不懈地做好网络与信息安全工作。

4.2 信息安全方针的原则

银行信息安全方针是组织的信息安全委员会或管理当局制定的一个高层文件，用于指导组织如何对资产（包括敏感信息）进行管理、保护和分配的规则和指示。

信息安全方针应当阐明管理层的承诺，提出组织管理信息安全的方法，并由管理层批准，采用适当的方法将方针传达给每一个员工。

信息安全方针应给信息安全工作提供清晰的指导方向，加强安全管理工作，保证业务系统的安全运营。

信息安全方针应适用于全体员工。

信息安全方针应当简明、扼要，便于理解，通常包括目标、范围、意图、法规的遵从性和管理责任等内容。

4.3 信息安全方针的主要内容

通常，银行信息安全方针包括信息安全定义、信息安全管理体系的范围、信息安全工作应遵循的基本原则、信息安全管理的目标和使命、信息安全管理体系实施、安全组织机构及职责、信息安全工作要求、信息安全方针维护等方面的内容。信息安全方针并没有一个统一的结构和内容，不同银行根据自身实际不同，其内容也有所差异。

以下是银行信息安全方针的一个示例。

某银行信息安全方针

经信息安全委员会审核通过，××××年××月××日通过

1. 信息安全定义

信息是一种资产，就像其他重要的业务资产一样，对于组织的业务是不可或缺的，因此需要妥善保护。信息可以以多种方式存在，可以打印或书写在纸张上，以电子文档形式存储，通过邮寄或电子方式传播，以胶片形式显示或在交谈中表达出来。

信息安全就是要保护信息的保密性、完整性、可用性及其他属性，如真实性、可核查性、可靠性、防抵赖性。

2. 信息安全管理体系的范围

信息安全管理体系通常适用于银行所有与软件开发、数据服务、信息技术基础设施及其他支持系统相关的业务活动。信息安全管理的范围是某银行信息技术部所负责管理和维护的，为关键业务流程提供信息技术支持相关资产。

3. 信息安全工作应遵循的基本原则

（1）“分级保护”原则 应根据各业务系统的重要程度及面临的风险大小等因素决定各类信息的安全保护级别，分级保护，合理投资。

（2）“同步规划、同步建设、同步运行”原则 安全建设应与业务系统同步规划、同步建设、同步运行，在任何一个环节的疏忽都可能给业务系统带来危害。

（3）“内外并重”原则 安全工作需要做到内外并重，在防范外部威胁的同时，加强规范内部人员行为和审计机制。

（4）“整体规划，分步实施”原则 需要对银行信息安全建设进行整体规划，分步实施，逐步建立完善的信息安全体系。

（5）“风险管理”原则 进行安全风险管理，确认可能影响信息系统的安全风险，并以较低的成本将其降低到可接受的水平。

（6）“适度安全”原则 没有绝对的安全，安全和易用性是矛盾的，需要做到适度安全，找到安全和易用性的平衡点。

（7）“三分技术、七分管理”原则 网络与信息安全不是单纯的技术问题，需要在采用安全技术和产品的同时，重视安全管理，不断完善各类安全管理规章制度和操作规程，全面提高安全管理水平。

4. 信息安全管理的目标和使命

通过信息安全管理，旨在确保银行信息技术部所有的信息资产的机密性、完整性和可用性，以及信息技术部基础架构、信息系统的连续性和可用性。为银行的业务应用提供安全、稳定、连续的信息技术支撑。

1）保障业务正常和安全运行，保证业务连续性。

2）保护客户隐私，保护客户资料的机密性，维护客户的利益。

3）保护银行的商业机密和技术机密，维护银行的利益。

5. 信息安全管理体系实施

银行信息技术部设立信息安全管理委员会来领导信息安全各项工作。

提高员工整体的信息安全意识，提高信息系统技术维护人员的安全技能水平和规范操作意识；所有员工都必须接受信息安全培训和教育，增强信息安全意识。

应该遵守各项法律法规要求，同时利用法律法规来保护银行信息技术部的利益。

应该选择适当的方法，识别并评估银行信息技术部面临的信息安全风险，并采取恰当措施予以处理。

建立有效的审核机制，加强对信息安全各项工作的监督与审核。

应该采取一套有效的安全事件管理机制，明确所有员工的安全责任，建立对已发生或可疑的信息安全事件的报告及响应流程，并对违反安全策略的人员进行惩罚。

6. 安全组织机构及职责

在信息安全方针中，可以对银行信息安全组织机构及职责进行简要描述，以对信息安全组织及人员安全管理部分进行指导。银行信息安全组织通常包括领导小组、工作小组、信息安全主管及安全员。

银行信息安全领导小组是由银行主管信息安全工作的高层领导主持，由银行信息安全主管与各部门主管组成的银行信息安全工作常设领导组织，是银行信息安全工作的最高决策机构和领导机构，全面负责银行信息安全各项工作。

银行信息安全工作小组是银行信息安全工作的执行机构，由银行信息安全主管担任组长，成员包括各部门安全管理员。

银行信息安全主管，由银行信息安全领导小组产生，具体负责信息安全管理的各项工作，并直接向信息安全领导小组汇报工作。

银行各部门安全管理员，由银行各部门产生，具体负责部门内部信息安全管理的各项工作，并直接向信息安全主管汇报工作。

7. 信息安全工作要求

银行和各部门必须建立和完善信息安全管理规章制度和操作程序，规范和加强信息安全管理工作，所有员工必须遵守与其相关的信息安全规章制度。

加强内部人员的安全管理，依据最小特权原则清晰划分岗位，在所有岗位职责中明确信息安全责任，要和工作岗位实现职责分离，关键事务双人临岗，重要岗位要有人员备份，定期进行人员的安全审查。

所有员工都应签署保密协议，并接受信息安全教育培训，提高安全意识，及时报告网络与信息安全事件。

必须加强第三方访问和外包服务的安全控制，在风险评估的基础上制定安全控制措施，并与第三方银行和外包服务银行签署安全责任协议，明确其安全责任。

各部门必须加强信息资产管理，建立和维护信息资产清单，维护最新的网络拓扑图，建立信息资产责任制，对信息资产进行分类管理和贴标签。

加强机房和办公区域的安全管理，为设备的正常运行提供物理和环境安全保障。

建立日常维护操作规程和变更控制规程，规范日常运行维护操作，严格控制和审批任何变更行为。

加强项目建设的安全管理，配套安全系统必须与业务系统“同步规划、同步建设、同步运行”，加强安全规划、安全审批、安全验收管理。

加强防范恶意软件，所有终端及服务器必须安装防病毒系统，定期更新病毒特征代码，及时报告发现的病毒。

按照补丁跟进和发布、补丁获取、补丁测试、补丁加载、补丁验证、补丁归档这一流程进行补丁安全管理。

建立维护作业计划，严格执行维护作业计划，加强对设备、操作系统、数据库、应用系统的运行监控，编写日常运行维护报告。

部署网络层面和系统层面的访问控制、安全审计及安全监控技术措施，保障业务系统的安全运行。

增强主机系统的安全配置，定期进行安全评估和安全加固。

制定各业务系统的应急方案，定期更新、维护和测试，做好数据备份工作，确保数据的及时恢复，保证数据的安全。

加强用户账号和权限管理，按照最小特权原则为用户分配权限，避免出现共用账号的情况。

加强用户口令的管理，口令长度至少 8 位，并采用数字、字母和特殊字符的组合，定期修改用户口令。

加强应用系统的安全管理，包括软件开发安全管理、投产测试和上线安全管理、应用软件版本和配置管理，加强外包开发的业务系统软件的安全管理。

建立安全检查制度和安全处罚制度，对违反规章制度的部门和人员按照规定进行处罚。

8. 信息安全方针维护

1）信息安全经理负责本方针的维护，并在方针执行期间提供支持。

2）各部门经理直接负责方针的执行，确保各部门员工都能遵守本方针。

3）信息安全方针必须强制执行。

4）本方针由银行信息安全管理委员会负责每年重新审订。

第 5 章
信息安全组织及人员安全管理

信息安全组织和人员信息安全管理是银行信息安全工作得以执行的基础。本章重点介绍了银行信息安全组织，包括信息安全组织的构建原则、架构、岗位和职责设计、信息科技部门与其他部门的关系。信息安全组织的落实需要靠银行各级人员在日常工作中对信息安全的遵守和支持，本章最后对人员安全管理进行了介绍。

5.1 银行信息安全组织的构建原则

银行信息安全组织的构建应充分体现其合规性、先进性及可操作性，因此在组织的构建过程中应充分考虑以下原则。

1）符合相关的国家法律法规及监管机构的要求。法律法规及监管机构的要求既是对安全组织构建的重要约束，同样在组织的构建过程中也能够体现重要的支撑支持作用，是银行信息安全组织能够有效落地的重要支撑。

2）能否达成集中政策、分级管理、专业分工、权责明晰的架构是信息安全组织能够高效运转的重要保障。

3）通过合规、审计、管理、执行等相关岗位的分离和相互制约的设计减少安全管理过程中的共谋风险。

4）通过条块结合的管理矩阵模式提升安全管理效率，体现信息安全管理的全面性。

5）运作机制借鉴国内外最佳信息技术治理实践。通过引入并应用国内外信息安全管理的最佳实践，实现信息安全管控工作的先进性。

5.2 银行信息安全组织的架构

基于上文所述的银行信息安全组织的构建原则，银行信息安全组织的构建从总体上

可采取以下的架构，即安全决策层、安全管理层、安全执行层、安全监管层（包括安全合规层、安全审计层）（图 5-1）。

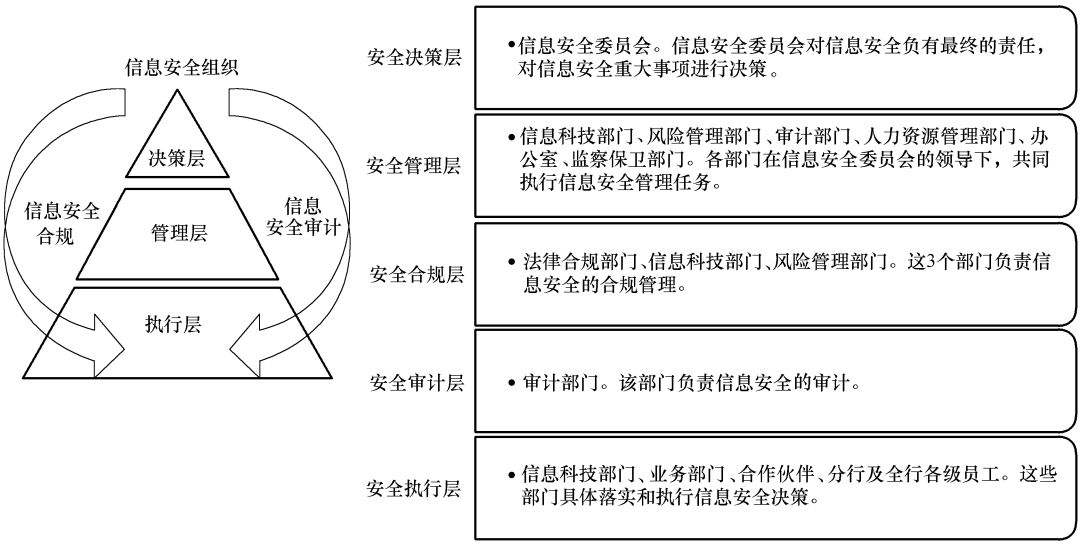


图 5-1　银行信息安全组织架构概览图

1. 安全决策层

不同银行在管理组织架构、治理结构、工作程序上存在一定的差异性，但从信息安全工作开展的原则上出发，为了便于信息安全工作在全行层面的有效推动开展并切实落地，建议设置独立的信息安全决策机构，如信息安全管理委员会，并酌情在其架构下设置信息安全工作小组。信息安全的决策层应定位为全行的信息安全决策机构，在决策层的组成上应纳入具备足够授权的高层管理者，建议的组成人员包括银行经营决策层分管科技的行领导、信息科技部门总经理、法律合规部门总经理、内审部门总经理，并结合银行管理组织架构、治理结构特点酌情纳入业务部门分管领导。

银行信息安全管理委员会及其下设工作小组建议的工作职责包括：

1）负责审议安全合规评估报告。

2）负责审议信息安全风险评估报告、信息安全风险管理工作报告。

3）审核重大信息安全风险的处置方案。

4）审核信息安全管理部门提交的与信息安全相关的策略、标准、总体规划、培训计划。

5）决策信息安全相关的重大事宜。

6）协调银行内信息安全组织内部，以及和其他部门之间的工作。

7）审核重大安全事件处理结果报告，并审批改进策略。

8）审议信息安全内审制度和年度审计计划、年度信息安全内部审计报告；督促已发现的安全审计问题的整改落实。

9）其他信息安全决策性工作。

2. 安全管理层

从提升银行信息安全管理效率的目的出发，通常在银行内规划设立专职的信息安全管理团队。在信息安全管理上，该安全团队应接受信息安全管理委员会的领导，并在其管理下开展信息安全相关管理工作。

1）安全管理层需要总体协调、推动信息安全各项管理工作。

2）组织搜集、整理并提供支持信息安全决策的相关数据、信息和资料。

3）审议银行内部信息安全管理的年度工作方案和工作计划。

4）每季度定期组织会议，制定全行信息安全制度及信息安全体系建设方案，监督、指导、评估、评价重大信息安全监管标准的遵从、落实、执行情况。

5）评估认定重大信息系统及信息安全事件造成的隐患、风险、损失和责任。

6）定期向信息科技部门报告信息安全战略规划的执行、信息安全整体状况及其他需要报告事项（图5-2）。

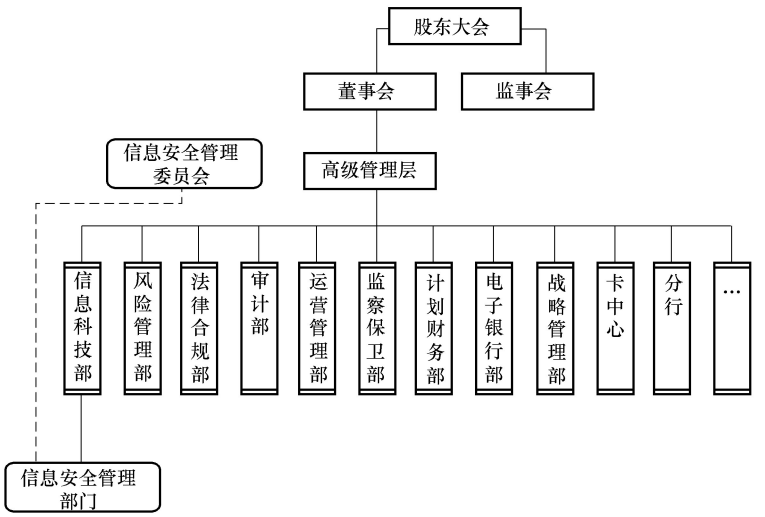


图5-2　安全管理层

3. 安全执行层

为了保障信息安全工作能够在全行范围内高效地开展，应明确识别与信息安全相关的岗位，确保其日常信息安全工作得以被指导、监控、检查、报告。从岗位分布看，可归类为信息科技条线信息安全执行岗位（如科技部门系统管理员等）与非科技条线信息安全执行岗位（如业务部门内设信息安全员岗位）。

4. 安全监督层

为了充分地保证信息安全工作监管的独立性，信息安全的监管类岗位通常在银行的内审部门进行设置，专职开展信息安全的日常审计工作；安全监督层需要监督全行运行系统操作规程、管理办法、实施细则、应急计划和控制技术等的实施；安全监督层还需要根据行内外信息安全形势，制订年度和专项信息安全检查计划，并且需要对信息安全

检查结果进行分析、总结，形成后续的信息安全工作方向的输入。

5.3 信息安全组织相关岗位及职责设计

上文对信息安全组织的构建进行了剖析，对各种信息安全管理组织的构建方式进行了横向的对比。银行在明确信息安全管理组织后，还应结合管理组织架构及信息安全管理开展的模式，配备相应的安全管理岗位、安全监管岗位、安全执行岗位人员，并明确其相应的安全职责。信息安全相关岗位如图 5-3 所示。

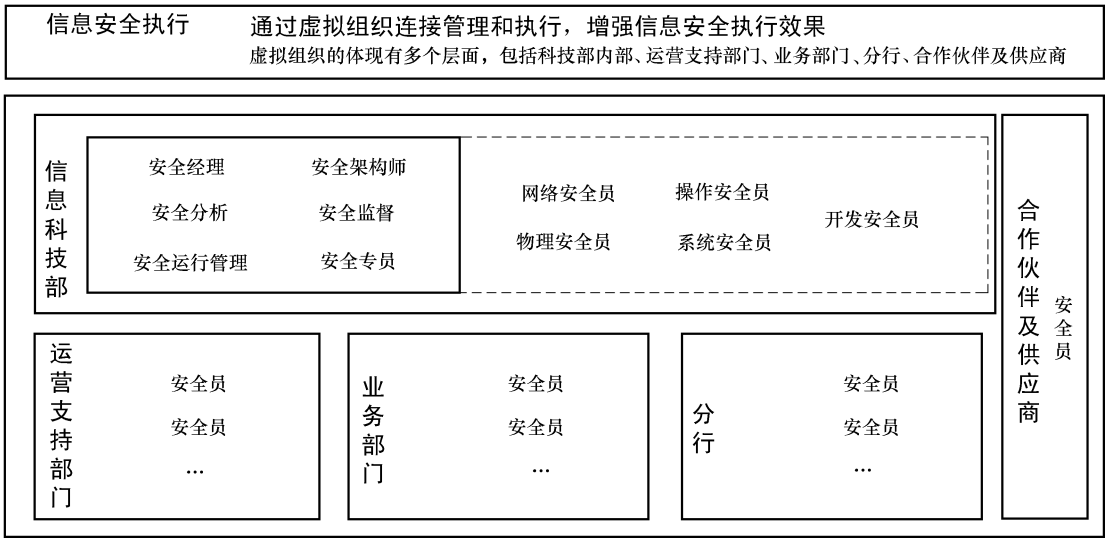


图 5-3 信息安全相关岗位示例图

在银行的信息安全管理实践中，还应结合实际的管理模式对岗位的汇报关系、工作职责、工作开展方式、工作职责界面、任职资格等加以明确的定义。下面将介绍典型的信息安全相关的岗位设置及其职责定义。

5.3.1 信息安全管理类相关岗位

（1）信息安全经理岗 负责信息安全管理在全行范围内的统筹开展。

1）组织全行的信息安全策略、管理标准、安全技术规范的制定、更新及培训。

2）代表信息安全管理部门向信息安全管理委员会上报信息技术安全策略、管理标准、安全技术规范。

3）负责全行的信息安全的整体规划，并监督实施。

4）组织评审项目的安全符合性。

5）组织调查和处理全行范围内重大信息安全事件。

6）组织制订信息安全风险评估、安全检查的年度计划。

7）组织进行信息安全风险评估和安全检查，提出风险控制或安全改进措施，并监督相关措施的执行。

（2）信息安全规划岗 负责制定安全策略、信息安全管理制度；监督检查信息安全管理制度的执行。

1）组织制定、更新全行信息安全管理制度、标准和管理流程。

2）组织全行的信息安全管理制度及流程的培训工作。

3）推动、监督、检查行内信息安全管理制度的执行。

4）负责与银行相关的第三方合作伙伴进行定期的安全交流，获得当前最新的安全管理方法和先进的安全管理经验。

5）参与银行安全的整体规划的制定，以及实施过程中的监督。

6）参与信息安全风险评估和重大信息安全事件的调查处理。

7）定期向信息安全经理提交本职工作报告及下一步工作的规划和安排。

8）参与制订全行的信息安全预算计划。

（3）信息安全设计岗 负责信息安全相关的技术架构，主要包括路由器、交换机、防火墙、入侵检测、主机服务器、数据库及中间件、中间件、应用软件等相关的实施及部署；以及对全行的信息安全技术执行情况进行监督、检查、支持。

1）组织制定、更新全行信息安全架构。

2）组织行内的信息安全技术规范的培训工作。

3）监督、检查行内信息安全技术规范的执行。

4）指导、监督软件开发中的安全技术手段和控制措施的符合性。

5）负责与相关的第三方合作伙伴进行定期的安全技术交流，获得当前最新的安全技术。

6）参与行内安全集成、安全服务、安全咨询项目的规划和项目开发中的安全技术和监督工作。

7）为信息安全审计人员提供合适的信息技术安全审计工具及技术支持。

8）定期向信息安全经理提交相关本职工作报告及下一步工作的规划和安排。

9）参与信息安全风险评估和重大信息安全事件的调查处理。

10）参与制订行内的信息安全预算计划。

（4）信息安全合规岗 根据国家的相关法律、法规对行内信息安全策略、制度、流程进行合规指导和监督；并为一些严重安全事件提供法律上的支持。

1）了解和信息安全相关的国内外法律、法规。

2）审核全行范围的相关信息安全策略、标准和流程的合规性，并提出修改建议。

3）定期向信息安全管理委员会提交行内的《信息安全合规报告》。

（5）安全员岗 为了保证信息安全在全行范围内能够有效地贯彻落实，通常在相关的组织部门内设置信息安全员岗位，参与信息安全策略、标准等管理制度的制定工作，制定并上报本职能范围的信息安全规划，负责推动和监督其所辖范围内的执行。

1）组织制定、更新全行信息安全架构。

2）根据需要参与信息安全策略、标准及技术规范的制定、改进及更新工作。

3）在总体安全规划下，按原有流程制定并上报本职能部门负责的信息安全规划、预算计划和培训计划。

4）组织推动信息安全规划、培训计划的实施。

5）负责所辖范围内的信息安全制度、技术安全培训工作。

6）及时就信息安全制度执行效果、反馈意见和有关重大隐患向信息安全管理经理反馈。

7）推动、监督所辖范围内信息安全制度的执行。

8）审批所辖范围内与信息安全相关的其他重要事项。

9）参与处理所辖范围内的重大信息安全事件。

10）定期编写所辖范围内的信息安全报告，并向信息安全经理提交报告。

5.3.2 信息安全执行类相关岗位

（1）安全执行管理岗 负责信息科技条线相关安全运维的管理工作。

1）负责制定全行科技的信息安全运行规划，包括服务器可用性保障规划，链路冗余规划，信息技术基础设备安全评估加固规划、备份规划及安全培训计划等。

2）组织实施各项规划内容，并负责监督、评估和改进。

3）组织相关安全操作规程、管理办法、实施细则、应急计划等的制定、更新，并向安全管理经理报备。

4）推动、监督全行运行系统操作规程、管理办法、实施细则、应急计划和控制技术等的实施。

5）组织相关人员参加信息安全制度、技术安全培训工作。

6）及时就信息安全制度执行效果、反馈意见和有关重大隐患向信息安全经理反馈。

7）定期提交《信息安全运行状况报告》。

8）负责组织进行信息安全的自我评估和自我完善。

9）配合调查和处理系统的重大安全运行事故或生产故障。

10）定期组织进行科技突发事件的应急演练，完善信息系统突发事件应急计划。

11）协助、检查其他安全专员安全制度的执行，如网络安全专员等。

12）协助、协调安全检查和调查工作。

（2）其他安全执行岗 包括系统安全岗、网络安全岗、应用安全岗、物理安全岗、数据安全岗、数据库安全岗、开发安全岗等。

1）各类组成岗位人员实际上隶属于银行信息科技部门的各个处室，只是在执行信息安全活动时接受信息安全管理部门的业务指导。

2）该类岗位的安全执行的职责主要为其所负责相关领域的信息安全标准的执行，相关信息安全事件的协助分析与报告，配合信息安全检查、信息安全审计工作的开展。

5.3.3 信息安全监督类相关岗位

（1）安全审计经理岗 负责统筹管理信息安全审计工作。

1）制订年度的信息安全内部审核工作计划及信息安全审计制度。

2）建立能进行审核工作的独立信息安全内审团队。

3）对信息安全审计过程中的质量控制负责。

4）对信息安全审计发现问题的改进措施进行跟踪。

（2）安全审计岗 负责信息安全审计工作的开展执行。

1）参与制定、更新信息安全内审制度。

2）参与制订信息安全总体审计计划。

3）执行年度信息安全内审计划并对信息安全审计工作进度和质量负责。

4）及时向信息安全审计经理反馈审计工作中发现的重大安全隐患。

5）定期向信息安全审计经理提交信息安全审计报告。

5.3.4 其他信息安全类岗位

其他信息安全类岗位如第三方信息安全顾问，是信息安全某些领域的专家（信息安全管理、信息安全技术等领域专家），合理地引入信息安全顾问服务可以作为银行信息安全管理实践过程中的有效补充，提升信息安全管理的成熟度。

5.4 安全部门与行内其他部门的关系定位

银行的信息安全组织需要有足够的力量去保证信息安全管理制度的有效实施。这尤其反映在与其他组织的协调、合作机制中。大量的实践表明，信息安全管理部门应当与以下组织建立起良好而有效的长期工作关系。

1. 业务部门

信息安全管理组织必须帮助和指导核心业务部门，确保应用系统的开发和修改符合业务流程的同时也满足信息安全的需求；并且协助业务部门发现、处理及解决安全事件；对相关员工进行安全职责教育。

2. 业务流程制定者

信息安全组织需要经常性地与业务流程制定者沟通，为他们提供信息安全方面的指导。业务流程负责人需要在每个科技开发项目的开始及整个生命周期过程中考虑信息安全。它包括在需求文档、服务质量协议和业务持续性计划中提出信息安全需求，确定风险。业务流程负责人决定谁可以创建、访问、修改或删除信息，通常是通过定义用户组

和授予相应的权限来实现的。

3. 办公室/行政部门/监察保卫部门

信息安全组织需要遵守办公室/行政部门/监察保卫部门关于物理安全方面的各项规定，协助完成物理安全保卫工作。

4. 人力资源管理部门

在信息安全意识培训、违背信息安全制度的处罚措施等方面，信息安全组织需要遵循人力资源管理部门的相关规定，并尽可能得到其支持。

5.5 人员安全管理

1. 内部人员

（1）雇佣过程 从信息安全观点看，雇佣员工的过程中存在较多潜在的信息安全隐患。安全管理人员应与人力资源部门员工建立相应的沟通合作机制，将信息安全因素作为人员雇佣过程中的重要考量。

在具体的实践中可考虑的安全控制主要为人员的身份背景调查。人员的身份背景调查应结合所招募岗位的安全敏感级别在实施的详细程度和深度上有所不同，如信息安全职位的候选人应该经历更为详细而全面的背景调查。

一些常见的背景调查包括身份核查、教育和证书检查、历史工作经验验证、信用历史核查（我国的信用管理体系正在逐步完善中，且已取得了较为长足的进展）、违法违规记录调查等。

（2）在职中

1）保密协议及信息资产访问授权确认。一旦候选人接受了工作，雇佣合同就成了重要的安全文件。在雇佣合同中可考虑部署信息安全相关的保密协议。另外，涉及针对应用信息系统或重要资源的访问，还可考虑要求员工签署针对信息资产访问/使用权限的授权确认。

2）安全意识提升、培训和教育。意识提升、培训和教育计划能够有效地改善员工的行为及使员工对他们的工作更有责任感。

在安全培训中应充分考虑针对不同岗位员工的信息安全教育的差异化，如针对安全专业人员的信息安全专业技能培训、信息科技人员的安全知识教育、一般员工与管理层的安全意识的培养教育之间的差异性。

安全意识提升作为最有效的安全提升方法，可以有效地纠正员工所有危害银行信息安全的行为。通过教导员工怎样正确地处理信息、应用信息，能够降低偶然损害或者信息破坏的风险性；通过让员工了解信息安全的威胁、这些威胁能够导致的潜在损坏及这些威胁发生的方式，降低因员工认为这些威胁不严重而带来的潜在风险；通过使员工了解策略、没有遵循策略将受到的惩罚和策略破坏被发现的机制，降低一个员工试图有意

错用和滥用信息的可能性。许多安全意识用较低的成本就可以开展，如录像、演讲、会议、海报、小册子、小饰物和布告牌等。

为了提升信息安全管理效应，银行还可考虑把信息安全纳入员工的业绩评估中。员工密切关注业绩评估，把信息安全任务包含进业绩评估可促使员工在执行任务时更加小心。

银行员工在职过程中的典型安全管理实践还包括采取双人控制、职责分离、职位轮换、强制休假等措施。

（3）人员解聘 在人员解聘过程中应主要考虑对员工访问信息的保护。具体的实践可考虑：

1）离任员工对信息系统的访问授权必须失效。

2）离任员工应确认归还所使用的信息资产，包括电脑、移动存储介质等。

3）应取消离任员工对银行职场、敏感区域的物理访问授权。

针对安全等级较高的岗位的员工的离职，还可考虑开展离职审查、签署保密协议等。

2. 外包服务人员

针对外包服务人员的管理，尤其是涉及银行敏感信息访问、信息资产访问的外包服务人员的管理与内部人员的安全管理较为相似，推荐针对外包服务人员的安全管理同样采取分阶段的形式来开展。同时，银监会在2013年颁布了《银行业金融机构信息科技外包风险监管指引》，其中也对外包人员的安全管理方面提出了相应的要求。

（1）提供服务前 银行人力资源管理部门应制定相应的筛选流程，其中应包含对外包服务人员在入场前进行背景检查（无犯罪记录、社保缴纳记录、技术能力与资质）的要求（咨询信息安全管理部门的意见）。该检查应与业务需求、已知风险相适宜，且相应筛选过程及结果应有记录文档。

（2）提供服务过程中 银行信息安全管理部门应与相应科技部门、人事管理部门、行政管理部门、法律合规部门等进行沟通，制定并部署与第三方服务人员相关的安全管控措施。相应的安全管控措施包括但不限于：

1）第三方服务人员相关的保密协议签署。

2）职场物理访问控制。

3）信息资产安全使用。

4）信息系统的授权访问管理。

5）第三方服务人员安全培训、安全教育。

6）第三方服务人员对银行安全要求遵从情况的评价。

7）第三方服务人员服务过程中自带办公软件的合规管理等。

（3）完成服务 在第三方服务人员完成相应的服务工作后，信息安全管理人员应重点关注其系统访问权限的回收、所使用银行信息资产的归还、工作交接过程等环节。

第 6 章
信息安全管理制度

为了加强银行信息系统安全保护工作，保障信息系统安全、稳定地运行，银行需要制定和遵守信息安全管理制度。信息安全制度的有效执行是银行信息安全工作的重点，也是难点。本章从银行信息安全工作实际出发，对信息安全管理制度的编写、实施、维护及信息安全制度集合进行描述。

6.1 文件化的信息安全管理

文件化管理模式是当前银行信息管理体系所普遍采用的。文件化管理模式主张在管理某项工作或活动时，应建立和实施程序，程序的执行需要保留可追溯的记录。通过文件落实责任、加强相关接口协调、提高工作的系统性和可追溯性，避免推诿扯皮，避免依赖经验、习惯，避免无章可依。

信息安全管理体系要求组织通过确定信息安全管理体系范围、制定信息安全方针、明确管理职责、以风险评估为基础，选择控制目标与控制方式等活动。信息安全管理体系一旦建立，银行应按体系规定的要求进行运作，保持体系运作的有效性。同时，应适当形成文件，即组织应建立并保持一个文件化的信息安全管理体系，来阐述被保护的资产、组织风险管理的方法、控制目标及控制方式和需要的保证程度。在银行进行信息安全管理的过程中，需要采用文件化的信息安全管理模式来开展相应的工作。

6.2 信息安全管理制度的编写

编写信息安全管理制度是组织建立体系化的信息安全管理的重要基础工作，也是一个组织实现风险控制、评价和改进信息安全管理、实现持续改进必不可少的过程。

在正式编写信息安全制度集合之前，银行应根据信息安全管理体系标准对文件化的

要求、对文件化程序的要求及信息安全管理活动策划的结果，列出信息安全管理所涉及的文件清单，不同层次的信息安全管理制度之间应保持衔接与协调一致。

银行业在编写信息安全制度时，力求制度能清晰描述安全控制或管理的责任及相关活动，能够回答 5W1H 六个问题，即目的与范围（Why）、做什么（What）、谁来做（Who）、何时（When）、何地（Where）及如何做（How）。回答这些问题一般不涉及技术性细节，并力求制度符合银行业务运作与安全控制的实际，具有可操作性，避免脱离实际而得不到贯彻执行。最好应该有安全制度编写小组或专门负责人员，协调各部门/团队的文件编写进度和内容把关，确保每个程序之间有必要的衔接，避免出现相互矛盾和责任真空。另外，在能够实现安全控制的前提下，信息安全制度的数量和每个制度的篇幅越少越好。

安全制度编写后可能需要经过多次的修改与完善；在正式发布实施之前，要对制度进行审核，确保符合信息安全管理相关标准与银行信息安全管理的实际；制度经过管理者批准后予以实施。在安全制度实施的过程中仍可对安全制度进行修订，但更改应按照制度控制程序所规定的方法进行，另外银行应保证员工在需要时可以获取制度。

6.3 体系化的信息安全制度及其框架模型

银行在信息安全管理过程中涉及大量的管理类文档和技术类文档，应根据安全文档使用的目的和发布范围，建立文档层级进行归类管理，以便查阅和调用，并形成一套有效的制度管理框架和工具。在此基础上根据制度层级确定每个制度文档编写、审批、发布的规则；确定文档密级和授权策略，规范文档被访问的原则。典型的制度层级框架如图 6-1 所示。

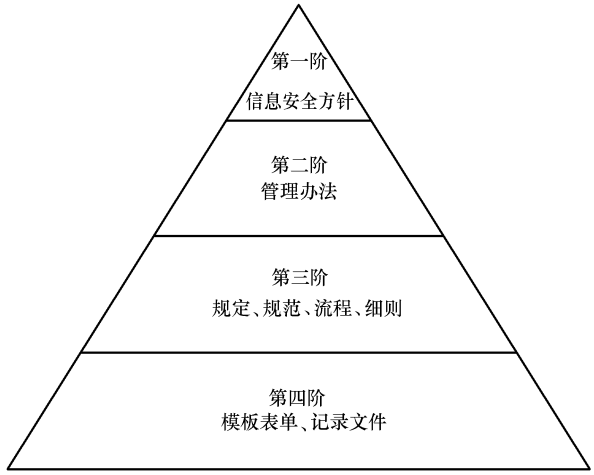


图 6-1 典型的制度层级框架图

1. 第一阶（信息安全方针）

信息安全方针是信息安全管理的最上层文件，也是信息安全的纲领性文件，其他文件如管理办法、流程、操作规范技术标准等，都必须遵从这些纲领性文件。

2. 第二阶（管理办法）

管理办法是信息安全管理制度的约束性文件，是对信息安全某一方面的原则性的规定。

3. 第三阶（规定、规范、流程、细则）

1）安全管理规定、细则是对管理办法的细化规定和要求。

2）安全规范是实现管理办法需要遵守的准则和规定，包括技术规范和管理规范。

3）安全流程是对管理办法的过程描述，侧重工作过程中输入、输出、活动、职责的界定。

4. 第四阶（模板表单、记录文件）

此阶为第一阶至第三阶文档制度在执行过程中用到的相关表单和记录。

6.4 信息安全制度文件的控制

1. 信息安全制度文件的控制总体要求

信息安全制度文件（包括记录）是银行重要的信息资产，为了规范对该类信息资产的保护，应建立文件化的程序来保证以下控制得到实施：

1）文件发布前得到批准，以确保文件是充分的。

2）必要时对文件进行评审、更新并再次批准。

3）确保文件的更改和现行修订状态得到识别。

4）确保在使用中可获得有关版本的适用文件。

5）确保文件保持清晰、易于识别。

6）确保外来文件得到识别。

7）确保文件的分发得到适当的控制。

8）防止作废文件的非预期使用。无论出于何种目的，如果需要保存作废的文件，应对这些文件进行适当的标识。

2. 安全制度的发布与评审

安全制度发布前的批准和更新后的再批准可以保证文件的“合法”地位，而且管理者从全局的角度来审视该文件，可以保证其充分性、可行性；安全管理层对文件的签署还可以提高文件的重视程度，便于文件的推行。

安全制度文件的评审可以保证文件的持续适宜性和充分性。通常在下列时机应该进行文件评审：

1）信息安全管理体系发生重大变化时。

2）信息安全管理体系标准发生重大变化时。

3）银行组织结构发生重大变化时。

4）信息系统发生较大变化、运作流程发生重大变化时。

5）重大安全事件发生后或者特定安全事件频繁发生时。

在信息安全制度发布前批准和更新后的再批准同样需要依据制度的不同类别明确相应的管理职责，表 6-1 为典型的针对不同制度类别进行管理职责定义的示例。银行在具

体的实践过程中，可以结合自身的治理模式、管理结构、安全工作开展形态对管理职责进行定义。

表 6-1　不同制度类别的管理职责定义示例

安全制度类别/层级	制(修)订/变更/作废	审　　核	批　　准	发 布 范 围
一阶制度	信息安全管理部门	信息安全管理经理	信息安全管理委员会	全行范围
二阶制度	信息安全管理部门	信息安全管理经理	信息安全管理委员会	全行范围
三阶制度	相关领域负责团队	专业条线负责人	信息安全管理经理	全行范围
四阶制度	相关领域负责团队	专业条线负责人	信息安全管理经理	全行范围

3. 安全制度的版本控制

内部文件版本的控制和外来文件的控制，可以保证信息安全管理文件使用者能够及时获得适当版本的文件，避免由于使用过期文件造成工作失误。对于纸面文件，通常的做法是在发放新文件的同时，收回旧版本的文件；同一版本内文件的更改，可以通过更改记录表清楚标识。对于电子文件需要根据组织具体的发布渠道和方式，采用适合组织实际情况的方法来控制，并且只要能够达到相关文件的控制要求即可。

4. 安全制度文件的密级管理及授权策略

作为银行内部较为敏感的一类信息资产类别，针对安全制度文件应采取授权访问的方式，通过明确定义文件的可访问级别，防止文件不必要的扩散所造成的安全隐患。

通常，信息安全制度文件的密级可定义为公开级、内部级和机密级。公开级文档密级最低，机密级文档密级最高。

1）公开级为常规性文档，所有人都有查阅的权限。

2）内部级为银行安全管理团队内部使用的资料，仅对银行安全管理团队内部员工提供查阅权限，若其他人员需要查阅相关文档，可以申请临时授权，经批准后才能查阅。

3）机密级文档为密级最高的文档，仅对银行管理层开放，对于非授权人员，可经过特殊授权获取临时查阅权限。

4）针对文档的访问授权，可以采取如下的方式：

① 临时授权：若需要查阅文档的人员不在文档发布范围之内，可以采用申请授权方式获得获取临时查阅文档的权限，如申请查阅内部级和机密级文档。

② 常规授权：若文档事先已确定其发布对象，可以采用常规授权的方式。

5. 安全制度文件的标识

针对信息安全管理文件其标识编码可采用六段可变位数进行描述，具体内容见表 6-2。

表 6-2　信息安全制度文件标识

XX Bank	Lm	XXYY	XXXXXX	Vn. n	XXYY
银行名称简写	制度层级	制度制定部门	制度中文名称	版本号	发布年月

1）第一段（XX Bank）代表银行的名称。

2）第二段（Lm，2 位字符）代表安全制度的阶层，m 分别取值 0、1、2、3。

3）第三段（XXYY，可变字符数）代表制度制定的部门。

4）第四段（XXXXXX，可变字符数）代表流程、规范、细则等制度文档的中文名。

5）第五段（Vn. n，固定 4 位字符）代表版本号，对于已经发布的版本都是 n. 0，中间版本的文件取 n. 1 ~ n. 9。

6）第六段（XXYY，固定 4 位数字）代表发布年月。

6.5 信息安全制度的贯彻实施

信息安全管理制度的发布，仅是银行信息安全管理工作开展的开端。此时，如何使这些制度文件贯彻到日常信息安全工作中去，成为银行信息安全管理人员的新课题。因为制定安全制定文件的目的不是为了束之高阁，也不是为了处罚员工（尽管处罚不可避免，但那也是为了保障信息安全管理运行），而是为了使信息安全管理得以有效开展，使银行的信息安全风险处于受控的状态，所以该问题的关键是，如何把信息安全制度准确地传达到每一位相关人员的日常工作中去，这需要很多方法配合使用。

例如，前面提到信息安全管理制度要经过管理层签署后发布，可以保证信息安全管理制度的地位，引起足够重视；文件版本控制可以保证员工总是能够及时得到最新的版本；而要求员工在文件生效之前签署一个文本，声明收到该版本的文件，并已经详细阅读、理解了其中的条款且愿意遵守这些文件，是为了引起员工的足够重视。

安全意识的培训也是把信息安全制度传达下去的一种好方法。培训可以形象而有针对性地让相关人员很快对信息安全制度形成整体的认识和比较深刻的印象，这是公文方式往往很难达到的效果。而且培训也是信息安全制度编写者和使用者的一次沟通，可以发现安全制度文件中一些容易产生歧义的字句，可以发现一些可能不符合实际情况的问题。

信息安全制度检查、信息安全审计工作的开展是信息安全制度得以实施的保障，要求银行必须定期对信息安全管控的运行情况进行检查与审计，验证银行内的信息安全管控是否有效实施，及时发现问题及时解决。

6.6 信息安全管理制度集合的组成

6.6.1 体系化的信息安全管理制度集合

信息安全制度的结构和内容应以安全管理要求为基础，并充分考虑国际标准 ISO/IEC 27001 及国家标准等级保护的相关要求，以符合业界共识。同时，也需要充分考虑

中国人民银行及银监会等监管机构的要求。

依据 ISO/IEC 27001，信息安全管理体系的文件至少应包括信息安全方针和安全目标的文件化声明；信息安全管理手册；风险评估报告；风险处理计划；组织为确保其信息安全过程有效策划、运作和控制所需的文件；ISO/IEC 27001 所要求的记录；实施的控制概要，包括任何删减理由的详细描述。对 ISO/IEC 27001 信息安全管理体系的贯彻实施，可以作为体系化银行信息安全管理制度的一个比较好的开端。

ISO/IEC 27001 提示不同组织的信息安全管理体系文件可能会因为组织的规模、类型、复杂度和安全要求的不同有所不同。组织可以依据标准、相关法律、法规、组织现行的安全控制规章制度和其他相关管理体系文件来确定自己体系文件的规模和组织方式。

1）信息安全方针：是信息安全目标、指标的框架，为信息安全活动建立方向和原则。方针必须强调法律法规的要求，为信息安全管理过程建立战略性的、全组织的风险管理环境。信息安全方针应该获得最高管理层的批准，是最高管理层对信息安全的总目标和对持续改进信息安全管理绩效的承诺。

2）信息安全管理手册：是组织信息安全管理体系的纲领性文件，是对组织信息安全管理框架的综述，阐明一个组织的信息安全方针并描述其信息安全管理体系的文件。信息安全管理手册对组织全体员工来说是法规性文件，必须严格遵照执行。信息安全管理手册应包括以下内容：信息安全管理体系的范围；支持信息安全管理体系的过程；为信息安全管理体系编制的程序文件，或对其引用。

3）风险评估报告：是风险评估的结论性报告，应该表述组织信息资产所面临的威胁、这些威胁能够利用的薄弱点及由此而产生的风险的大小优先等级。

4）风险处理计划：是组织针对所识别的每一项不可接受风险建立的详细处理方案和实施时间表，是组织安全风险和控制措施的接口性文档。为了管理和审核的方便，这个计划通常还会罗列已经采取的控制措施。

5）组织为确保其信息安全过程有效策划、运作和控制所需的文件：这部分文件在其他管理体系中一般叫程序文件和作业指导性文件，是规定如何完成某项活动的方法的文件。程序文件和作业指导性文件在内容的范围上有一点细微的区别，程序文件通常是用来协调多个部门共同完成一项任务，而作业指导性文件通常用来指导个别岗位或部门内的活动。

6）记录：在管理体系中一般把记录作为一种特殊的文件来看待，是表述达到的结果或者提供活动完成的客观证据，是管理体系持续改进的见证人。记录应该体现信息安全管理体系全部过程的业绩，以及发生的与信息安全管理体系相关的所有安全事故。在不违反法律法规和标准的要求前提下，组织可以根据自身对记录的需求和记录缺乏带来的风险决定记录的内容和详略。

6.6.2 对监管要求的整合落实

信息安全工作，应该既对银行本身具有价值，又能够满足监管要求，也就是有价值、又合规。因此在信息安全制度制定的过程中，应充分地整合相应的监管要求。针对

银行业，应积极地分析并在制度中着重落实银监会的监管要求、中国人民银行信息安全管理相关的政策指引、金融标准委员会及其他政府机构与信息安全相关的策略与标准。另外针对部分上市银行还应考虑其特定的合规性的要求，部分境外上市银行还应将境外的监管要求融入其信息安全管理制度中。

6.6.3 某商业银行信息安全制度文件目录示例

以下是某商业银行信息安全制度包含的文件：

信息科技风险管理政策
信息科技风险管理制度
信息安全管理策略
信息系统安全管理机构
信息安全岗位设置及人员配备管理规范
电子银行业务信息安全管理指引
数据安全管理办法
应用系统密钥管理办法
运维中心安全访问管理细则
内部用户动态令牌管理细则
移动存储介质使用管理规定
网络安全管理规范
互联网边界入侵检测管理细则
桌面 PC 使用管理细则
桌面管理系统管理细则
恶意代码防范管理规范
统一身份与访问管理系统使用管理细则
身份与访问管理系统应用接入管理规范
信息安全检查规范
应用系统数字证书管理规范
数据调用管理规范
加密接口使用管理规范
应用系统密钥管理实施细则
生产系统业务数据修改实施细则
办公电子文件防泄密系统管理细则
信息安全产品和安全服务采购规范
安全监控管理规范
系统测试与验收管理规范
分行信息安全管理规范

第 7 章
信息安全风险管理

信息安全风险管理是信息安全运作的核心组成部分。从本质上看，信息安全运作是通过日复一日的信息安全活动，发现、缓解、监控和报告风险，并对信息安全风险进行控制。另一方面，信息安全风险管理本身作为一种日常的信息安全活动是信息安全运作的一种形式。

本章基于国际国内不同标准、规范对信息安全风险管理的不同阐述，对银行业信息安全风险管理进行了分析。在此基础上，本章较为系统地分析了信息安全风险管理的含义、银行业信息安全风险管理的流程、信息安全风险评估、信息安全风险处置及信息安全风险评估实践等内容。

7.1 信息安全风险管理的不同含义

通常，风险是指发生损失的不确定性或损失出现的概率；也可以指某些特定损失发生的可能性。在某些情境下，风险甚至可以解读为事件可测定的不确定性，包括不确定性的收益或损失。在不同的语境中，风险往往拥有不同的含义。

7.1.1 国际通用标准对风险的定义

2007 年 4 月 22 日 ~ 27 日，国际标准化组织技术管理局风险管理工作组（ISO/TMB/WG Risk Management）在加拿大渥太华召开了第四次工作组会议。正式将风险定义为不确定性对目标的影响。

7.1.2 《巴塞尔协议》对风险的划分

巴塞尔银行监管委员会（Basel Committee on Banking Supervision，BASEL）简称巴

塞尔委员会，是由美国、英国、法国、德国、意大利、日本、荷兰、加拿大、比利时、瑞典十大工业国的中央银行于1974年底共同成立的，作为国际清算银行的一个正式机构，以各国中央银行官员和银行监管当局为代表，总部在瑞士的巴塞尔。每年定期集会4次，并拥有近30个技术机构，执行每年集会所订目标或计划。

自成立以来，巴塞尔委员会制定了一系列重要的银行监管规定，如1983年的银行国外机构的监管原则，又称巴塞尔协定（Basel Concordat）和1988年的巴塞尔资本协议（Basel Accord）。这些规定不具有法律约束力，但十国集团监管部门一致同意在规定时间内在十国集团实施。经过一段时间的检验，鉴于其合理性、科学性和可操作性，许多非十国集团监管部门也自愿地遵守了巴塞尔协定和资本协议，特别是那些国际金融参与度高的国家。1997年，有效银行监管的核心原则的问世是巴塞尔委员会历史上又一项重大事件。核心原则是由巴塞尔委员会与一些非十国集团国家联合起草的，得到世界各国监管机构的普遍赞同，并已构成国际社会普遍认可的银行监管国际标准。至此，虽然巴塞尔委员会不是严格意义上的银行监管国际组织，但事实上已成为银行监管国际标准的制定者。

2002年10月1日，巴塞尔委员会发布了修改的资本协议建议的最新版，同时开始新一轮调查（第三次定量影响测算，QIS3），评估该建议对全世界银行最低资本要求的可能影响。从1975年9月第一个《巴塞尔协议》到1999年6月《新巴塞尔资本协议》（或称“新巴塞尔协议”）第一个征求意见稿的出台，再到2006年新协议的正式实施，时间跨度长达30年。几十年来《巴塞尔协议》的内容不断丰富，所体现的监管思想也不断深化。

最新通过的《巴塞尔协议Ⅲ》受到了2008年全球金融危机的直接催生，该协议的草案于2010年提出，在短短一年时间内就获得了最终通过，并于当年11月在韩国首尔举行的G20峰会上获得正式批准实施。《巴塞尔协议Ⅲ》是国际清算银行（BIS）的巴塞尔银行业条例和监督委员会的常设委员会——巴塞尔委员会于1988年7月在瑞士的巴塞尔通过的“关于统一国际银行的资本计算和资本标准的协议”的简称。该协议第一次建立了一套完整的国际通用的、以加权方式衡量表内与表外风险的资本充足率标准，有效地扼制了与债务危机有关的国际风险。《巴塞尔协议Ⅲ》几经波折，最终于2013年1月6日发布其最新规定。新规定放宽了对高流动性资产的定义和实施时间。

《巴塞尔协议Ⅲ》是全球银行业监管的标杆，其出台必将引发国际金融监管准则的调整和重组，影响银行的经营模式和发展战略。在《巴塞尔协议Ⅲ》出台之际，中国银监会及时推出了四大监管工具，即资本要求、杠杆率、拨备率和流动性要求，及时进行了跟进，构成了未来一段时期中国银行业监管的新框架。这被业界称为中国版“巴塞尔Ⅲ”。

《巴塞尔协议》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、法律风险及战略风险八大类。

无论是巴塞尔委员会，还是《巴塞尔协议》，都没有对信息安全风险及信息安全风

险管理进行定义和详细叙述。银行业通常认为，站在《巴塞尔协议》角度来看，商业银行信息安全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。

7.1.3 国际标准 ISO/IEC 27005 对信息安全风险的描述

国际标准 ISO/IEC 27005：2008 对信息安全风险的定义是：某种特定的威胁利用资产或一组资产的脆弱点，导致这些资产存在受损或破坏的潜在可能，通常用事态的可能性及其后果的组合来测量。

ISO/IEC 27005 认为，信息安全风险管理过程可能循环进行风险评估和/或风险处置活动。风险评估的循环方法能够使得每一次循环更加深入和具体，循环方法可以在确保高风险被准确识别和识别控制措施上花费最小的时间与精力之间寻找平衡。首先确定范畴，然后进行风险评估。如果风险评估为进行有效决策的提供了充分的信息，以确定将风险降低到可接受级别所需活动，则风险评估任务结束，可开始进行风险处置。如果信息不够充分，则进行另外一个修订范畴和风险评估的循环，也可能是整个范围内的部分内容进行循环。

有效的风险处置依赖于风险评估的结果。风险处置可能不会立即将残余风险降低到可以接受的级别。对于这种情形，可能需要变更风险范畴参数（如风险评估、风险接受或影响的准则）以再次进行风险评估循环，并可能需要进一步的风险处置。风险接受活动需要确保残余风险被组织的管理者明确接受。对于控制措施被取消或推迟实施（如成本问题）的情形，管理层的明确接受就更为重要。在整个信息安全风险管理过程中，向相应的管理者和员工传达风险及风险的处置是很重要的。甚至在风险处置前，有关已识别的风险信息对于管理事件可能是很有价值的，并可以帮助降低潜在损失。管理者和员工的风险意识、降低风险的现有控制措施的特性及组织所关心的区域，将为处理事件和非预期事态提供有效的帮助。信息安全风险管理过程的每一活动及两个风险决策点的详细结果应该形成文件。

7.1.4 国家标准 GB/Z 24364 及 GB/T 20984 对信息安全风险的定义和说明

国家标准 GB/Z 24364—2009《信息安全技术信息安全风险管理指南》与 ISO/IEC 27005 的基本思路保持了一致，其将风险定义为：由于系统存在的脆弱性，人为或自然的威胁导致安全事件发生的可能性及其造成的影响。风险由安全事件发生的可能性及其造成的影响这两种指标来衡量。

GB/T 29084 对信息安全风险的定义为：人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。同时，GB/T 29084 对信息安全风险评估进行了定义，即依据有关信息安全技术与管理标准，对信息系统及

由其处理、传输和存储信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

从上述分析可以看出，不同的标准对信息安全及信息安全风险管理的定义不尽相同，但不同标准的整体思路和核心内涵是一致的。银行在进行信息安全管理时，应该综合考虑、参考和借鉴上述标准规范的思路。而国际标准 ISO/IEC 27005 及国家标准 GB/Z 2364、GB/T 20984 是站在信息技术的角度看待信息安全，其描述也更为详细，可以作为银行业信息安全风险管理主要参考的标准。

7.2 银行信息安全风险管理过程

7.2.1 基于 ISO/IEC 31000 的风险管理过程

ISO/IEC 31000 从一个组织通用的风险管理角度出发，阐述了一个组织风险管理的原则和指导方针，并给出了风险管理原则、框架和过程的关系图，并对其中风险管理过程进行了详细描述，如图 7-1 所示。

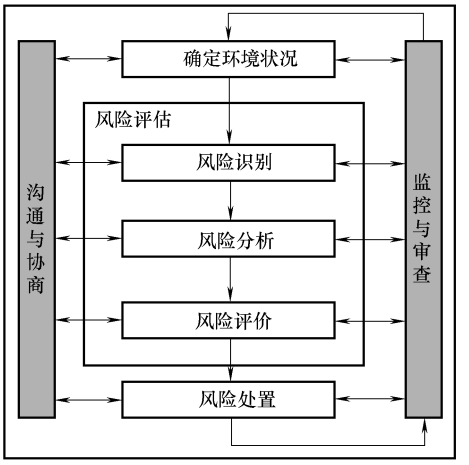


图 7-1 ISO/IEC 31000 风险管理过程

7.2.2 基于操作风险的风险管理过程

从操作风险管理的角度，银行往往将风险管理划分为风险识别、风险评估、风险控制/缓释、风险监测/报告等过程。

7.2.3 基于 ISO/IEC 27005 的风险管理过程

ISO/IEC 27005 指出，信息安全风险管理过程由确定范畴、风险评估、风险处置、风险接受、风险沟通及风险监视和评审组成（图 7-2）。

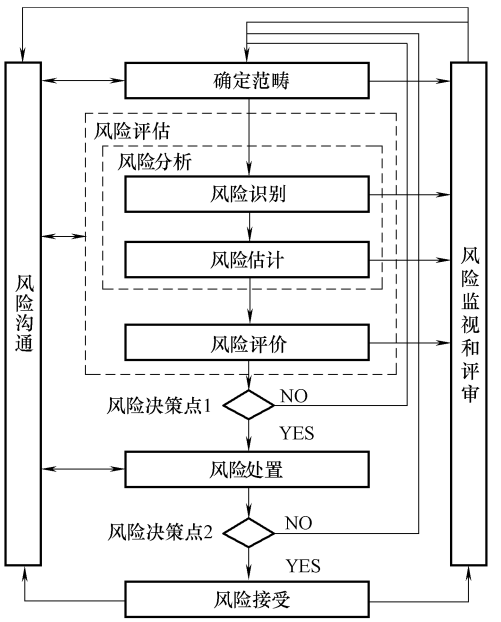
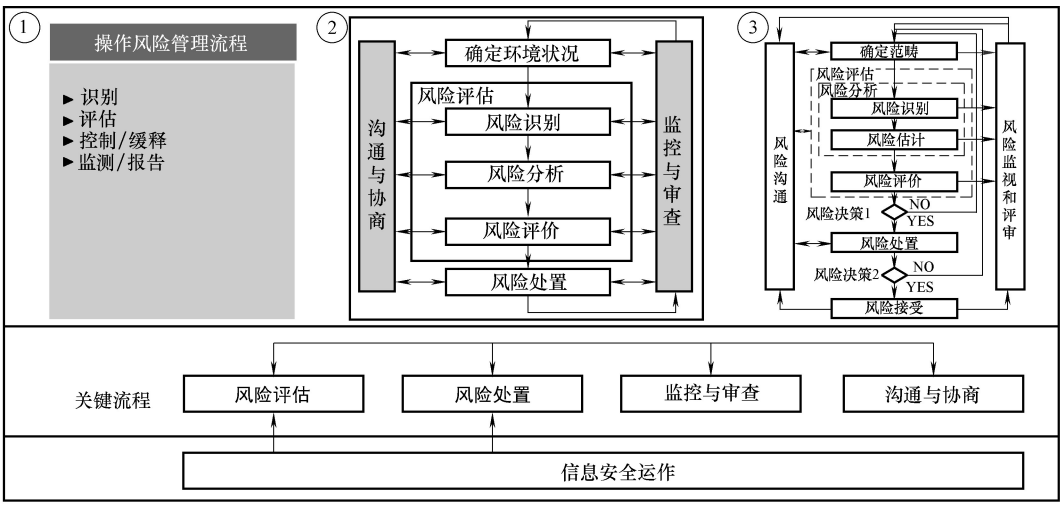


图 7-2 基于 ISO/IEC 27005 的风险管理过程

ISO/IEC 27005 中最为关键的 3 个部分是风险评估、风险处置及基于风险的决策。风险评估过程将全面评估信息系统的资产、威胁、脆弱性及现有的安全措施，分析安全事件发生的可能性及可能的损失，从而确定信息系统的风险，并判断风险的优先级，建议处理风险的措施。风险处理过程基于风险评估的结果，考察信息安全措施的成本，选择合适的方法处理风险，将风险控制到可接受的程度。基于风险的决策是风险管理的决策过程，旨在由信息系统的主管者或运营者判断残余风险是否处在可接受的水平之内。基于这一判断，主管者或运营者将做出决策，决定是否允许信息系统运行。

7.2.4 银行信息安全风险管理的关注重点

综上所述，无论基于哪种标准，风险管理的核心理念都是相通的，即通过基本的风险管理过程对风险进行管理。银行风险管理工作本身也是一种体系化的工作，即银行风险管理体系。信息安全管理体系和风险管理体系之间既有交叉融合，又有区别和不同。站在信息安全管理体系的角度，重点关注信息安全风险评估与信息安全风险处置，因为它们是信息安全管理体系的基础，如图 7-3 所示。



注:①来自于银行操作风险管理流程;②来自于ISO 31000—2009,③来自于ISO 27005—2008

图 7-3　银行信息安全风险管理关注重点

7.3　银行信息安全风险评估

7.3.1　风险评估基本概念

基于 ISO/IEC 27005 对信息安全风险的定义，有几个概念需要明确，见表 7-1。

表 7-1　ISO/IEC 27005 中与信息安全风险相关的术语及定义

术语	定　义
资产	任何对组织具有价值的东西,包括计算机硬件、通信设施、建筑物、数据库、文档信息、软件、信息服务和人员等,所有这些资产都需要妥善保护
资产价值	经济实体所拥有的固定资产、无形资产能够给企业带来的潜在经济收入、效率提升,或失去这些固定资产、无形资产可能给企业带来的损失
威胁	可能对资产或组织造成损害的某种安全事件发生的潜在原因
弱点	也被称作漏洞或脆弱性,即资产或资产组中存在的可被威胁利用的缺点,弱点一旦被利用,就可能对资产造成损害
风险	特定威胁利用资产弱点给资产或资产组带来损害的潜在可能性
风险评估	风险分析和风险评价的整个过程,包括系统地使用信息来识别风险来源和估计风险,以及将估计的风险与给定的风险准则加以比较,以确定风险严重性的过程
风险处置	选择并且执行措施来更改风险的过程
残余风险	经过风险处置后遗留的风险

在银行的实际业务经营过程中，上述风险管理各要素的相互作用方式如图 7-4 所示。

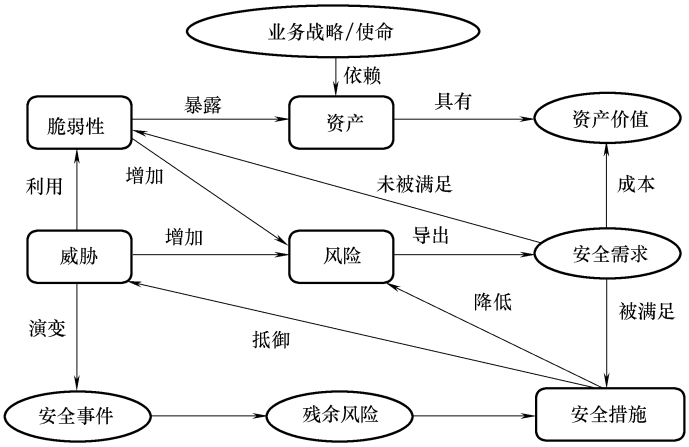


图 7-4　信息安全风险管理要素的相互作用

1）业务战略的实现对资产具有依赖性，依赖程度越高，要求其风险越小。

2）资产是有价值的，组织的业务战略对资产的依赖程度越高，资产价值就越大。

3）风险是由威胁引发的，资产面临的威胁越多则风险越大，并可能演变成为安全事件。

4）资产的脆弱性可能暴露资产的价值，资产具有的脆弱性越多则风险越大。

5）脆弱性是未被满足的安全需求，威胁利用脆弱性危害资产。

6）风险的存在及对风险的认识导出安全需求。

7）安全需求可通过安全措施得以满足，需要结合资产价值考虑实施成本。

8）安全措施可抵御威胁，降低风险。

9）残余风险有些是因安全措施不当或无效，需要加强才可控制的风险；而有些则是在综合考虑了安全成本与效益后不去控制的风险。

10）残余风险应受到密切监视，它可能会在将来诱发新的安全事件。

7.3.2　风险评估过程

银行业一般采用图 7-5 所示的风险评估的实施流程。

1. 风险评估的准备

风险评估的准备是整个风险评估过程有效性的保证。银行实施风险评估是一种战略性的考虑，其结果将受到组织业务战略、业务流程、安全需求、系统规模和结构等方面的影响。

2. 资产识别

资产是具有价值的信息或资源，是安全策略保护的对象。它能够以多种形式存在，

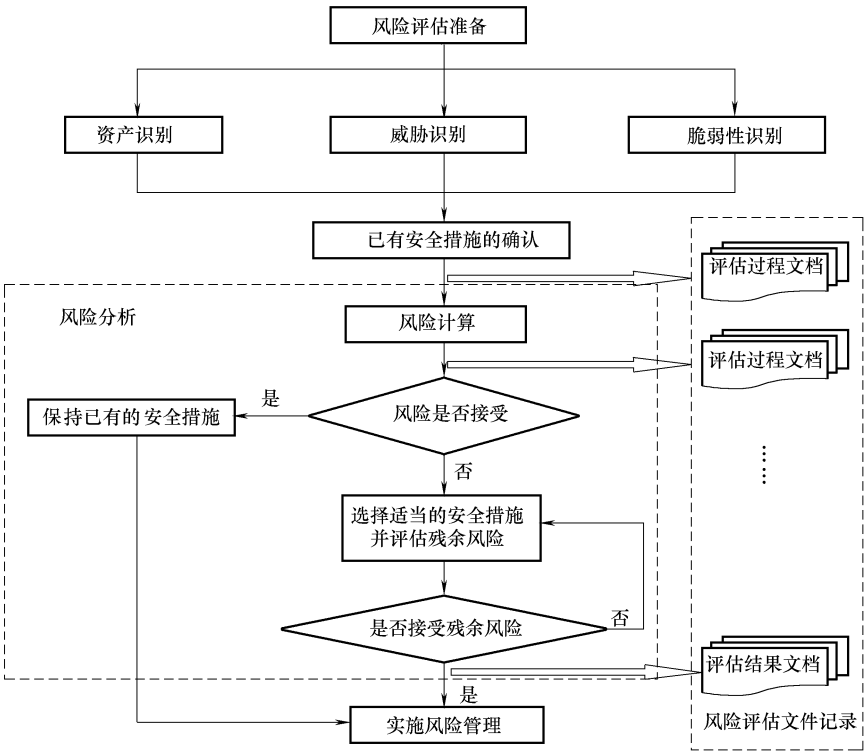


图 7-5　风险评估实施流程图

有无形的、有形的，有硬件、软件，有文档、代码，也有服务、形象等。机密性、完整性和可用性是评价资产的 3 个安全属性。信息安全风险评估中资产的价值不仅仅是以资产的账面价格来衡量，还由资产在这 3 个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定的。安全属性达成程度的不同将使资产具有不同的价值，而资产面临的威胁、存在的脆弱性，以及已采取的安全措施都将对资产安全属性的达成程度产生影响。

3. 威胁识别

威胁是一种对银行及其资产构成潜在破坏的可能性因素，是客观存在的。造成威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和无意两种。环境因素包括自然界中不可抗的因素和其他物理因素。威胁作用形式可以是对信息系统直接或间接的攻击，如非授权的泄露、篡改、删除等，在机密性、完整性或可用性等方面造成损害，也可能是偶发的或蓄意的事件。

4. 脆弱性识别

脆弱性是对一个或多个资产弱点的总称。脆弱性识别也称为弱点识别，弱点是资产本身存在的，如果没有相应的威胁发生，单纯的弱点本身不会对资产造成损害。而且如果系统足够强健，再严重的威胁也不会导致安全事件，并造成损失。即威胁总是要利用资产的弱点才可能造成危害。

资产的脆弱性具有隐蔽性，有些弱点只有在一定条件和环境下才能显现，这是脆弱性识别中最为困难的部分。需要注意的是，不正确的、起不到应有作用的或没有正确实施的安全措施本身就可能是一个弱点。

脆弱性识别将针对每一项需要保护的资产，找出可能被威胁利用的弱点，并对脆弱性的严重程度进行评估。脆弱性识别时的数据应来自于资产的所有者、使用者，以及相关业务领域的专家和软硬件方面的专业等人员。

脆弱性识别所采用的方法主要有问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。

5. 已有安全措施的确认

银行应对已采取的安全措施的有效性进行确认，对有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。对于确认为不适当的安全措施，应核实是否应被取消，或者用更合适的安全措施替代。

安全措施可以分为预防性安全措施和保护性安全措施两种。预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性，如入侵检测系统；保护性安全措施可以减少因安全事件发生对信息系统造成的影响，如业务持续性计划。

已有安全措施的确认与脆弱性识别存在一定的联系。一般来说，安全措施的使用将减少脆弱性，但安全措施的确认并不需要与脆弱性识别过程那样具体到每个资产、组件的弱点，而是一类具体措施的集合。比较明显的例子是防火墙的访问控制策略，不需要描述具体的端口控制策略、用户控制策略，只需要表明采用的访问控制措施。

6. 风险分析

（1）计算安全事件发生的可能性 根据威胁出现频率及脆弱性状况，计算威胁利用脆弱性导致安全事件发生的可能性，即：

安全事件发生的可能性 = L(威胁出现频率,脆弱性) = L(T,V)

在具体评估中，应综合攻击者技术能力（专业技术程度、攻击设备等）、脆弱性被利用的难易程度（可访问时间、设计和操作知识公开程度等）及资产吸引力等因素来判断安全事件发生的可能性。

（2）计算安全事件发生后的损失 根据资产重要程度及脆弱性严重程度，计算安全事件一旦发生后的损失，即：

安全事件的影响 = F(资产重要程度,脆弱性严重程度) = F(Ia,Va)

部分安全事件的发生所造成的影响不仅仅是针对该资产本身，还可能影响业务的连续性。不同安全事件的发生对银行造成的影响也是不一样的，在计算某个安全事件的损失时，应将对银行的影响也考虑在内。

（3）计算风险值 根据计算出的安全事件发生的可能性及安全事件的损失，计算风险值，即：

风险值 = R(安全事件发生的可能性,安全事件的损失) = R[L(T,V),F(Ia,Va)]

评估者可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法。

通过构造经验函数，矩阵法可形成安全事件发生的可能性与安全事件的损失之间的二维关系；运用相乘法可以将安全事件发生的可能性与安全事件的损失相乘得到风险值。

7. 风险评估文件记录

对于风险评估过程中形成的相关文件，还应规定其标识、储存、保护、检索、保存期限及处置所需的控制。相关文件是否需要及详略程度由管理过程来决定。

7.3.3 风险评估结果报告

风险评估的结果报告对后续的风险处置工作意义重大。风险评估中必须确定信息系统的安全风险状况（包括风险级别、风险点等），但这不能作为风险评估的全部结论。

除风险状况外，在风险评估工作的结果报告中还应包括以下的报告：

1）信息系统体系特征报告。

2）威胁评估报告。

3）脆弱性评估报告。

4）安全措施分析报告。

上述报告分别在风险评估的各项步骤中生成，并与风险状况报告合并作为最终的风险评估结果报告。其中，威胁评估报告应与脆弱性评估报告相对应，指出威胁可能会利用的脆弱性（即威胁/脆弱性对）。基于该报告，评估者应对安全措施做出建议。

7.3.4 管理风险评估中引入的新风险

与信息系统脆弱性有关的信息、信息安全保障的现状和问题等是涉及银行要害、利益、声誉的重大事项，因此风险评估是敏感的工作。如果处理不当，风险评估会带来新的风险，从而使信息系统的风险有可能比不评估还要大。

此外，风险评估有可能影响到信息系统应用的正常进行，发生意外损失，甚至直接造成安全事件。

为此，在风险评估时，应缜密设计评估方案，考察风险评估过程中可能引入的新风险。尤其在进行委托评估时，应选择有资质和有能力的风险评估机构，评估前应签署慎重的评估合同，评估过程中注意对人员的监督和评估数据的保护，评估结束后应妥善处理评估现场，禁止评估数据随意带出。

7.4 风险评估的关键内容说明

银行信息安全风险评估是对信息资产价值、面临的威胁、存在的弱点及三者综合作用而带来风险的可能性和影响的评估。在风险评估过程中，对威胁信息资产的可能性、严重性的取值定义及风险处置措施的制定从以下几个方面考虑：

1）要确定需要保护的信息资产的范围及具体信息资产，明确信息资产的直接和间接价值。

2）确定信息资产面临的潜在威胁，威胁发生的可能性有多大。

3）确定信息资产中存在的可能会被威胁所利用的弱点，以及利用的容易程度。

4）确定一旦威胁事件发生，给银行带来的操作风险、法律风险、信誉风险。

5）对识别出的信息科技风险，银行应采取相应的风险处置措施将信息安全风险带来的损失降低到可接受的程度。

总的来说，银行风险评估应关注定量与定性的评估方法、信息资产的分类和分级、威胁的分类和分级、资产弱点的严重性、风险的计算等关键内容。

7.4.1 定量与定性的评估方法

信息安全风险评估方法有两种：定量的方法和定性的方法。定量分析是试图从财务价值上对构成风险的各项要素（特别是资产）进行量化分析评估的一种方法，由于定量分析所依赖数据的可靠性和有效性很难保证，加之对数据统计缺乏长期性，所以，定量分析的方法在银行信息安全风险评估中并不常用，取而代之的是更容易实施的定性分析方法。定性风险评估并不一定要对构成风险的各个要素（特别是资产）进行精确的量化评价，它借助评估者的经验判断、业界惯例及银行自身定义的标准，来对风险要素进行相对的等级分化，最终得出的风险大小，只需要通过等级差别来分出优先顺序即可。事实上商业银行最关心的是业务活动的持续性，对于影响业务活动持续性的各种风险问题，在有限的资源支持情况下，只需要抓住最突出的问题，有针对性地采取措施即可。

信息安全风险评估是依据有关的政策法规及商业银行相关信息技术标准，对系统及由其处理、传输和存储信息的保密性、完整性和可用性等安全属性进行综合评估的活动过程。风险评估包括对信息资产的弱点、信息资产面临的威胁及其发生的可能性，以及弱点被威胁利用后所产生的负面影响，并根据安全事件发生的可能性和负面影响的程度来标识信息资产的安全风险。风险评估模型如图 7-6 所示。

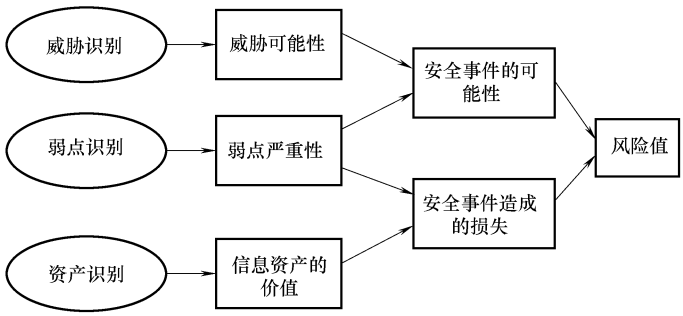


图 7-6　风险评估模型

注：该图来源于《GB/T 20984—2007. 信息安全风险评估规范》。

在风险评估模型中，主要包含信息资产等级、弱点、威胁和风险 4 个要素，每个要素有各自的属性。信息资产的属性是资产价值；弱点的属性是弱点被威胁利用后对资产带来影响的严重程度；威胁的属性是威胁发生的可能性和历史发生频率；风险的属性是风险值的高低。因此风险评估及管理的过程是：

1）对信息资产进行分类，依据资产在不同安全属性（保密性、完整性及可用性）中所占权重的不同对资产进行赋值。

2）识别信息资产的弱点，并对弱点的严重程度赋值。

3）对威胁进行评估，并对威胁发生的可能性和历史发生频率赋值。

4）计算信息资产的风险值，得到信息资产的风险级别，并对风险进行处置，选择合适的控制措施。

风险评估的结果是在对现有安全控制措施执行有效性评估的基础上，将评价得出的资产价值、威胁可能性和弱点严重性分别赋值，将三者赋值相乘，计算得出最终的风险值。

7.4.2 信息资产的分类和分级

信息资产是指任何对企业具有价值的信息资产，包括计算机硬件、通信设施、建筑物、数据库、文档信息、软件、信息服务和人员等，所有这些资产都需要妥善保护。为了进一步定义其价值，一般需将其分类，除一般认可的软件、硬件、数据资产外，还需增加人员、服务等项目，在此基础上可进一步细分，以达到精细化管理的要求。

结合相关标准（如 ISO/IEC 27005 等）、“三道防线”及相关法规（如《商业银行信息科技风险管理指引》《商业银行内部控制指引》等）的要求，可以将信息技术资产分为硬件类、软件类、数据/文档、组织、人员、服务及网络七类。然后根据资产类别、职能或等级划分为不同子类，并根据其所支持的业务或实现的功能划分小类，从而实现资产的三级分类（表 7-2）。

表 7-2 信息资产分类

类　别	子　类	资产类别编号	资 产 简 介
硬件	服务器	HW1—1	核心业务区服务器
		HW1—2	非核心业务区服务器
		HW1—3	灾备类服务器
		HW1—4	开发/测试主机
	物理环境设备	HW2—1	电力及空调设施
		HW2—2	安防设施
	桌面终端设备	HW3—1	桌面终端
	其他	HW4—1	备份存储介质

（续）

类　别	子　类	资产类别编号	资 产 简 介
软件	应用系统软件	SW1—1	业务系统
		SW1—2	渠道类软件
		SW1—3	管理类软件
		SW1—4	数据类软件
	服务器类软件	SW2—1	数据库软件
		SW2—2	服务器操作系统软件
	终端类软件	SW3—1	终端操作系统软件
数据/文档	机密信息	DT1—1	机密类数据文档
	秘密信息	DT2—1	秘密类数据文档
	内部信息	DT3—1	内部数据文档
组织	信息安全治理层	ORG1—1	风险及审计委员会
	信息安全管理层	ORG2—1	信息科技管理委员会及信息安全管理小组
	信息安全执行层	ORG3—1	信息技术部
		ORG3—2	业务部门
		ORG3—3	其他一般执行部门
人员	管理类人员	PS1—1	部门负责人
	内部一般岗位人员	PS2—1	程序开发人员
		PS2—2	程序测试人员
		PS2—3	运行维护人员
		PS2—4	一般岗位人员
	第三方人员	PS3—1	外包商人员
		PS3—2	清洁人员、保安、物业人员、电工等
网络	网络设施	NW1—1	网络基础设施
		NW1—2	安全设备及设施
服务	电信类服务	SVC1—1	电信网络类服务
	人员类服务	SVC2—1	外包人员服务
	基础类服务	SVC3—1	物业服务

对细分后的信息资产，需定义其价值。这里所讲的价值并不是财物价格，而是从信息安全的角度，即机密性、完整性、可用性的价值取值，可采取三级分类。资产价值评估主要对资产的保密性（C）、完整性（I）、可用性（A）进行赋值评估。在评估过程中，对所有的资产都进行了 CIA 赋值，并依据资产的自身特点，细化了其保密性、完整性、可用性的适用范围，比如硬件类资产安全属性应关注可用性（硬件的保密性、完整性不适用），根据实际情况和业界经验，针对每类资产，制订了资产 CIA 适用范围，如表 7-3 所示。

表 7-3　资产 CIA 赋值

资产类别	CIA 适用范围	CIA 赋值等级
硬件	A—可用性	1—低、2—中、3—高、4—极高
软件	C—保密性 I—完整性 A—可用性	1—低、2—中、3—高、4—极高
数据/文档	C—保密性 I—完整性 A—可用性	1—低、2—中、3—高、4—极高
组织	C—保密性 I—完整性 A—可用性	1—低、2—中、3—高、4—极高
人员	C—保密性 I—完整性 A—可用性	1—低、2—中、3—高、4—极高
网络	C—保密性 I—完整性 A—可用性	1—低、2—中、3—高、4—极高

通过前面对信息技术资产安全属性的赋值，可以判断该资产在公司安全风险管控活动中的价值，经过价值等级计算，公司就可以结合相应的弱点/威胁等级对资产采用明确的分类保护措施，从而达到保障公司信息技术经营活动的目标。信息技术资产等级的计算主要来源于资产的 3 个属性，同时参考最佳实践并根据企业特点，通过以下公式对资产价值进行计算。

$$\text{资产价值} = \text{Round1}\{\text{Log2}[(A \times 2^{\text{Conf}} + B \times 2^{\text{Int}} + C \times 2^{\text{Ava}})/3]\}$$

式中，A 代表保密性的权值；B 代表完整性的权值；C 代表可用性的权值；Round 函数是按制定位数，对数值四舍五入（Round1 表示保留 1 位小数）。

计算出信息技术资产安全价值大小后，可将它分为以下 4 个等级（表 7-4）。

表 7-4　资产等级

资产等级	价值分类	资产价值
1	低	0—1(含 1)
2	中等	1—2(含 2)
3	高	2—3(含 3)
4	很高	3—4(含 4)

7.4.3　威胁的分类和分级

风险评估过程中，针对不同的威胁来源，我们考虑了下述的安全威胁种类。

1）不可抗力、不可控且不为意志转移的威胁事件，如台风等环境灾难、鼠蚁虫

害、火灾等。

2）人为错误与人员相关的威胁事件，如失误导致的数据丢失、错误的操作、无意造成的损害等。

3）技术故障物理设备及基础设施等出现的技术或功能故障，如网络组件故障、供电故障等。

4）蓄意破坏公司内部或外部人员有意识的对信息资产造成的破坏事件，如偷窃、伪装、社会工程等。

威胁的可能性是指威胁事件发生概率或频率的定性描述。威胁的可能性赋值主要需考虑其历史发生频率及现有管控措施下的安全事件发生的可能性。本方法将威胁可能性分为 3 个等级，分别是高、中、低，将其从高到低分别赋值 3 ~ 1 分。威胁赋值标准参照表 7-5。

表 7-5　威胁赋值及定义

威胁赋值	等级	描述	威胁值定义
3	高	很可能	威胁能利用弱点而造成冲击的可能性高，且该威胁的历史发生频率很高
2	中	可能	威胁能利用弱点而造成冲击的可能性中，且该威胁的历史发生频率中或较高；威胁能利用弱点而造成冲击的可能性中等或较高，且该威胁的历史发生频率中等
1	低	不太可能	威胁能利用弱点而造成冲击的可能性很低；或者该威胁的历史发生频率很低或未发生过

7.4.4　资产弱点的严重性

弱点评估是资产风险评估中的主要内容。弱点是资产本身存在的，可被威胁利用，进而引起信息资产的损失。本次风险评估过程中考虑的弱点是针对硬件、软件、数据/文档、组织、人员和网络六种资产的弱点。

弱点评估的主要目的是评估信息资产的弱点严重性。此次弱点评估所使用的主要方法包括：

1）信息技术安全扫描：使用漏洞扫描工具对应用系统所在环境及开发测试所在的网络环境进行安全扫描，结果作为风险评估输入内容的一部分。

2）人员问询：询问相关人员，以了解信息资产风险的实际情况，并在工具中进行记录。

3）集体评估：和相关人员进行共同讨论，就信息资产风险评估过程中的赋值及结论达成共识。

4）文档查阅：查阅相关文档，以了解信息资产安全相关的管理手段。

弱点的严重性主要是指弱点被利用所引发影响的严重程度。本次风险评估过程中将弱点严重性分为 3 个等级，分别是高、中、低，将弱点严重性从高到低分别赋值 3 ~ 1

分。弱点赋值标准参照表 7-6。

表 7-6　弱点赋值及说明

弱点赋值	等级	说明(当该弱点被利用时引起后果的严重性)
3	高	缺乏相应的管控标准,且未执行相应的控制措施,以至于该弱点被利用后造成的影响很高
2	中	设计了相应的管控标准,但不够完善或执行过程中没有严格合规,以至于该弱点被利用造成的影响中等
1	低	设计了完善的管控标准,且执行有效,以至于该弱点被利用造成的影响有限或可忽略

7.4.5　风险的计算

前文已经指出，每项资产的风险状况可用公式简单计算得到，即

风险值 = 资产价值 × 威胁可能性 × 弱点严重性

资产价值分为 4 类的情况下，其价值高低取值分别为 4、3、2、1；威胁可能性、弱点严重性采用三级分类的情况下，其高、中、低取值分别为 3、2、1，资产的风险值则可参照表 7-7。

表 7-7　信息安全风险计算

风险级别	下限值	上限值
高(H)	24	36
中(M)	9	18
低(L)	1	8

可以定义风险值为 1 ~ 8 的资产为低风险资产，风险值为 9 ~ 18 为中等风险资产，风险值为 24 ~ 36 为高风险资产。

银行可根据自身的风险偏好，确定可接受的风险程度，如低风险可接受，而中高风险不可接受；然后对不可接受风险采取相应的控制和降低措施（可参考 ISO 27001 信息安全管理体系标准业务的相关策略）。通常通过降低风险发生的可能性，确保所有资产的残余风险控制在可接受的范围内。

7.5　银行信息安全风险处置

7.5.1　风险处置方式

消除所有风险往往是不切实际的，也是不可能的，必须在权衡成本的前提下实现最合适的风险处置措施，将风险控制在可接受的级别，使得可能的负面影响最小化。风险

处置包括对风险评估过程中建议的安全措施进行优先级排序、评估和实施。

风险处置是一种系统化方法，可通过多种方式实现：

1）风险承受：接受潜在的风险并继续运行信息系统，不对风险进行处理。

2）风险降低：通过实现安全措施来降低风险，从而将脆弱性被威胁源利用后可能带来的不利影响最小化（如使用防火墙、漏洞扫描系统等安全产品）。

3）风险规避：不介入风险，通过消除风险的原因和/或后果（如放弃系统某项功能或关闭系统）来规避风险。

4）风险转移：通过使用其他措施来补偿损失，从而转移风险，如购买保险。

在选择风险处置方式时应该考虑银行的目标和使命。不可能解决所有的风险，应对那些可能给使命带来严重危害的威胁/脆弱性对进行优先级排序。同时，在保护单位的使命及其信息系统时，由于各单位有其特定的环境和目标，因此用来处理风险的方式和实现安全措施的方法也各有不同。

7.5.2 风险处置的针对性

风险处置方式及安全措施体现了极强的针对性，必须依靠风险评估的结果确定风险处置方式及具体的安全措施。

在安全措施中，有的针对信息系统中的脆弱性（如为系统漏洞打补丁），有的针对威胁（如使用物理隔离手段，使攻击者无法访问系统）。威胁的属性包括威胁的主体（威胁源）、能力、资源、动机、途径、可能性和后果。在针对威胁的措施中，可视具体情况，针对不同的威胁属性，采用不同的手段来处理。

1）针对威胁源：采用物理隔离手段，使攻击者无法访问系统，消除威胁源。

2）针对威胁者的能力：采用强加密手段，使一般攻击者无法解密重要信息。

3）针对威胁者的资源：采用层次化的保护和纵深防御措施，使攻击者的资源难以支持其突破信息系统的保护防线。

4）针对威胁者的途径：将通信线路和电源线路置于墙内或天花板内，防止被老鼠咬断。

7.5.3 风险处置的过程

在处理风险时，可遵循以下步骤，旨在解决最大的风险，以最小的成本来将风险控制在可接受的水平，同时使风险对其他使命能力的影响降至最小。

（1）步骤 1 对优先级进行排序。基于在风险评估结果报告中提出的风险级别，对风险处置的工作进行优先级排序。高等级（如被定义为“非常高”或“高”风险级的风险）的风险项应该最优先处理。

步骤 1 的输出：从高优先级到低优先级的行动。

（2）步骤 2 评估所建议的安全措施。风险评估过程中建议的安全措施对于具体的

单位及其信息系统可能不是最适合和最可行的。在该步骤中，要对所建议的安全措施的可行性（如兼容性、用户接受程度）和有效性（如保护程度和风险控制的级别）进行分析，旨在选择出最适当的安全措施，使风险降至最低。

步骤 2 输出：可行安全措施的列表。

（3）步骤 3 实施成本效益分析。为了使管理层做出决策，并找出成本有效性最好的安全措施，要实施成本分析。

步骤 3 输出：成本效益分析的结果，判断实现或拒绝一个安全措施时的成本和效益。

（4）步骤 4 选择安全措施。在成本效益分析的基础上，选择成本有效性最好的安全措施来降低单位的风险。

步骤 4 输出：所选择的安全措施。

（5）步骤 5 分配责任和任务。遴选出拥有合适的专长和技能，可实现所选安全措施的人员（包括单位内部的人员或外部服务商/集成商），并赋以相应责任。

步骤 5 输出：责任和任务人员清单

（6）步骤 6 制订安全措施的实现计划。在本步骤中将制订安全措施的实现计划。该计划应该至少包括下列信息：

1）风险（脆弱性/威胁对）和相关的风险级别（风险评估报告的输出）。

2）所建议的安全措施（风险评估报告的输出）。

3）优先的行动（将高优先级赋予“非常高”或“高”风险级的项目）。

4）所选择的预期安全措施（基于可行性、有效性、机构的收益和成本来决定）。

5）实现预期安全措施时所需的资源。

6）负责小组和人员清单。

7）开始日期。

8）目标完成日期。

9）维护要求。

步骤 6 输出：安全措施的实现计划。

（7）步骤 7 实现所选择的安全措施。根据责任和任务分配，调动资源实现所选择的安全措施，但安全措施实施后仍然存在的风险为残余风险。

步骤 7 输出：残余风险清单。

7.5.4 风险处置的成本分析

为了有效分配资源并实现成本有效性较好的安全措施，在确定所有可能的安全措施并对其可行性和有效性进行评估后，应对每一个建议的措施进行成本效益分析，以判断哪些措施是必需的且适合于用户的环境。

成本效益分析可以是定性或者定量的，其目的是说明安全措施的实现成本相对于风险级的降低来说是合理的。

对所建议的安全措施进行成本效益分析时，可包括以下内容：

1）判断由于实现安全措施而带来的影响。

2）判断由于没实现安全措施而带来的影响。

3）对实现安全措施的成本进行估计。包括但不限于：

① 购买硬件和软件的成本。

② 如果因为安全措施而导致系统性能或功能下降，所降低的运行效率是多少。

③ 制定并实施安全策略和流程的成本。

④ 新增工作人员来实现安全策略、流程或服务的成本。

⑤ 培训成本。

⑥ 维护成本。

⑦ 针对资产价值而对实现成本和可能产生的效益进行评估，以判断在给定的成本和相应的影响下，新的安全措施对单位的必要性和重要性。

银行的管理层必须判断哪些才是可接受的风险。当一个单位确定可接受的风险范围后，才可能去评估安全措施的影响，包括实现和不实现安全措施带来的影响。这一风险范围因不同的单位而有所不同；然而，判断是否使用新的安全措施时可利用下列规则：

① 如果安全措施对风险的降低效果比预期的要求还要好，则应考虑是否有更廉价的替代方案。

② 如果安全措施的成本超过它所能降低的风险，则应寻找其他方法。

③ 如果安全措施没有降低风险，则寻求更多的安全措施或另外一种不同的安全措施。

④ 如果安全措施能够降低风险并且成本有效性比较好，则选用它。

一般而言，实现一项安全措施的成本比不实现一项安全措施的成本更容易确定。因此，高级管理层在判断是否要实现安全措施时扮演着关键的角色。

7.5.5 残余风险管理

残余风险是指采取安全措施对风险进行处理，提高了信息安全保障能力后，仍然可能存在的风险。残余风险的来源为两方面，一部分残余风险来自于安全措施可能不当或无效，以后需要继续控制这部分风险；另一部分则是在综合考虑了安全的成本与资产价值后，有意未去控制的风险，这部分风险是可以被接受的。

残余风险应受到密切监视，因为它可能会在将来诱发新的事件。风险处置的最后过程中，应列举出信息系统中所有残余风险的清单。在信息系统的运行中，应密切监视这些残余风险的变化，并及时处理。再次评估信息系统安全风险时，应将残余风险作为重点。

第 8 章
信息安全规划与建设

信息安全规划与建设、信息安全监控与检查、信息安全事件与应急响应、业务连续性与灾难恢复，以及信息安全审计等是信息安全运作的主体内容。它们之间紧密联系，相互协调，构成了信息安全运作的闭环管理。

本章重点介绍了信息安全规划与建设的内容，包括信息安全规划的意义、定位、要求、主要任务，信息安全规划的内容、主体与时间，信息安全规划的形式。与信息安全规划密切相关的是信息安全建设，本章重点介绍了信息安全建设的原则、依据、内容等。

8.1 信息安全规划

8.1.1 信息安全规划的意义

信息安全规划在信息安全运作甚至整个信息安全管理体系具有重要意义，它包括：

1）战略落地需要：信息安全战略的有效执行，需要将信息安全战略上升到国家战略的高度，同时，还需要通过信息安全战略规划，保障信息安全战略有效落地执行。

2）规范信息安全体系：通过信息安全规划，将信息安全进行系统性研究，形成合理的信息安全体系，保障信息安全工作的全面性和合理性。

3）指导信息安全工作开展：对信息安全重点内容进行规划，有利于指导具体工作的开展。

4）加强信息安全宣传：信息安全规划同时也是对信息安全本身的一种宣传，让全行各级领导和各级员工加强信息安全意识。

8.1.2 信息安全规划的定位

从银行业务战略、科技战略和信息安全的定位上看，科技战略承接和支撑业务战

略，信息安全承接和支撑科技战略。因此信息安全规划应以强化信息科技风险防范和信息安全保障能力，提供业务持续、稳定、健康发展为最终目标（图 8-1）。

信息化规划是以整个银行的发展目标、发展战略和银行各部门的业务需求为基础，结合行业信息化方面的需求分析、环境分析和对信息技术发展趋势的掌握，定义出银行信息化建设的远景、使命、目标和战略，规划出银行信息化建设的未来架构，为信息化建设的实施提供一幅完整的蓝图，全面系统地指导银行信息化建设的进程。信息安全规划依托银行信息化战略规划，对信息化战略的实施起到保驾护航的作用。信息安全规划的目标应该与银行信息化的目标一致，而且应该比银行信息化的目标更具体明确、更贴近安全。信息安全规划的一切论述都要围绕着这个目标展开和部署。

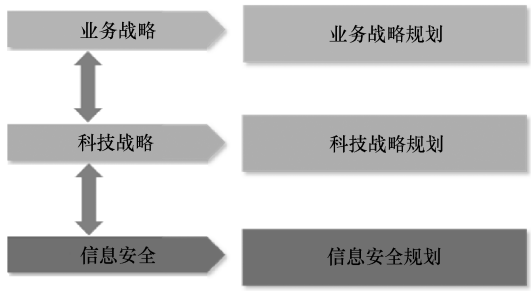


图 8-1　银行信息安全规划定位

8.1.3　信息安全规划的要求

信息安全规划的最终效果应该体现在对信息系统与信息资源的安全保护上，因此规划工作需要围绕着信息系统与信息资源的开发、利用和保护工作进行，包括蓝图、现状、需求、措施 4 个方面。首先，对信息系统与信息资源的规划需要从信息化建设的蓝图入手，明确银行信息化发展策略的总体目标和各阶段的实施目标，制定信息安全的发展目标；第二，对银行的信息化工作现状进行整体的、综合的、全面的分析，找出过去工作中的优势与不足；第三，根据信息化建设的目标提出未来几年的需求，这个需求最好可以分解成若干个小的方面，以便于今后的落实与实施；第四，要将实施工作阶段的具体措施与办法文档化，提高规划工作的执行力度。

信息安全规划服务于银行信息化战略目标，信息安全规划做得好，银行信息化工作的实现就有了保障。信息安全规划是银行信息化发展战略的基础性工作，不是可有可无，而是非常重要的。由于银行信息化的任务与目标不同，所以信息安全规划包括的内容就不同，建设的规模就有很大的差异，因此信息安全规划无法从专业书籍或研究资料中找到非常有针对性的帮助，也不可能给出一个规范化的信息安全规划的模板。在这里提出信息安全规划框架与方法，给出了信息安全规划工作的一种建设原则、建设内容、建设思路，具体规划还需要深入细致地进行本地化的调查与研究。

8.1.4　信息安全规划的主要任务

1. 夯实信息安全基础，推进信息资产分类分级管理

1）以国家等级保护制度为基础，建立重要系统安全防护体系和技术管理体系，建

立主动防御机制。

2）逐步推进信息资产识别和分类、分级工作，建立信息资产分级标准、规范，明确安全策略和保护要求。

3）落实管理责任，统筹推进信息安全管理工作，确保信息安全管理范围的全面覆盖。

4）加强敏感信息保护，防止信息资产违规泄露，加强向外部提供信息的统一管理，严格审核，归口发布。

5）综合运用技术和管理手段，加强终端设备的安全管理。

2. 强化系统建设各环节的安全管控，加强安全质量管理

1）建立和完善信息系统生命周期安全管理机制，加强信息安全管理制度体系建设，覆盖信息安全方针、策略、管理要求、操作流程、应急计划和联动机制。

2）加强信息系统建设全过程安全管理，制订信息安全规划，建立信息安全架构，统一部署信息安全功能，提高安全措施效率。

3）加强需求与设计阶段安全功能需求分析与设计，抓好安全测试工作并贯穿系统研发过程，检测安全漏洞，评估安全需求的符合性。

4）加强上线前安全评估，评价系统安全性及对整体安全保障体系的影响。

5）加强系统运行安全评审，及时发现并处置安全隐患。

3. 优化信息安全技术防控手段，实现纵深防御

1）优化信息安全技术防御体系，在物理安全、网络安全、系统安全、应用安全、数据安全、操作安全等不同层面，完善身份认证、访问控制、资源管理、日志分析、操作审计等安全功能，主动应对安全威胁，重点防范外部攻击，提升信息安全保障体系的健壮性和有效性。

2）强化基础设施安全保障，深化应用系统安全建设，增强应用产品安全性。

3）建立用户认证和访问控制管理流程，加强数据访问权限管理，有效保护信息资产。

4. 建立信息安全保障能力评价机制，保障信息安全管理有效性

1）建立信息安全保障体系评价机制，确定量化指标，及时开展评估、审计。

2）建立持续改进机制，保障信息安全管理的持续性、有效性。

8.1.5 信息安全规划的内容、主体与时间

规划内容解决“规划什么”的问题，可分为信息安全战略规划、信息安全体系规划和信息安全重点内容规划三大部分。信息安全战略规划是对信息安全从战略高度进行的阐述和规划，信息安全体系规划是对安全体系全局性的规划，对信息安全体系的组成、结构、相互关系进行系统分析和说明，信息安全重点内容规划是对信息安全的某一具体内容的详细规划，如信息安全架构规划、信息安全专题规划等。

规划主体解决“谁来规划”的问题，规划主体为银行本身。但其规划任务可由外部机构承担。对于信息安全战略规划和信息安全体系规划，建议由外部咨询公司承担，而内部人员起到管理和统筹的作用。对于信息安全重点内容的规划，可由外部咨询机构或者内部人员承担。内部人员在外部规划的基础上，结合自身能力，进行信息安全规划的执行、调优及评价。内部安全规划职责可以不单独设岗，但职责需明确在某一岗位上。

规划时间解决“什么时候规划”的问题，对于信息安全战略规划及信息安全体系规划，建议每 3 ~5 年定期进行，对于重点内容的详细规划，建议根据需要择机进行。

8.1.6 信息安全规划的形式

信息安全规划的方法可以不同，侧重点也可以不同，但是需要围绕技术安全、管理安全、运维安全等进行全面的考虑。规划的内容基本上应该涵盖：确定信息安全的任务、目标、战略及战略部门和战略人员，并在此基础上制订出物理安全、网络安全、系统安全、运维安全、人员安全的信息安全总体规划。物理安全包括环境设备安全、信息设备安全、网络设备安全、信息资产设备的物理分布安全等；网络安全包括网络拓扑结构安全、网络访问安全等；系统安全包括操作系统安全、应用软件安全、应用策略安全等；运维安全应在控制层面和管理层面得到保障，包括备份与恢复系统安全、漏洞检查及系统补丁功能、口令管理等；人员安全包括安全管理的银行机构、人员安全教育与意识机制、人员招聘及离职管理、第三方人员安全管理等。

信息安全规划的形式包括信息安全战略规划、信息安全体系规划及信息安全重要内容规划，如图 8-2 所示。

1. 信息安全战略规划

进行信息安全战略规划，通过规划进行详细的信息安全战略分解，对于信息安全愿景、目标、关键指标、管理层承诺、战略实施方法及信息安全战略如何落实业务战略和科技战略等内容进行系统阐述。

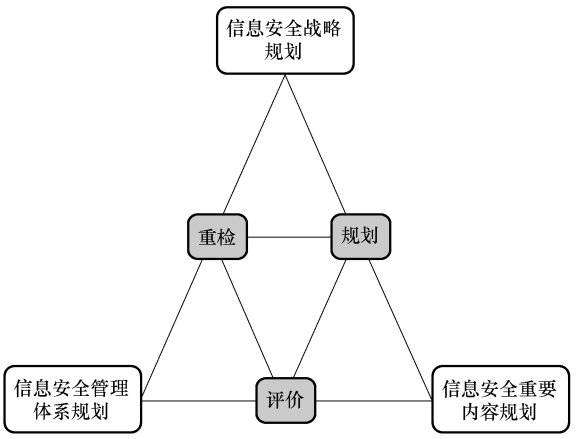


图 8-2 信息安全规划的形式

1）规划内容：信息安全愿景、目标、关键指标、管理层承诺、战略实施方法及信息安全战略如何落实业务战略和科技战略。

2）承担主体：外部机构为主。

3）规划期限：每 3 ~5 年定期进行。

4）规划要点：形成专门的信息安全战略规划制度，保证其执行。在战略规划前进

行安全战略的重检。每年年初对规划内容进行细化分解，年末对规划的执行情况进行评价。

2. 信息安全管理体系规划

1）规划内容：信息安全管理体系的组成、结构、相互关系。

2）承担主体：外部机构为主。

3）规划期限：每 3 ~ 5 年定期进行。

4）规划要点：形成专门的信息安全体系规划制度，保证其执行。在体系规划前进行安全体系的重检。每年年初对规划内容进行细化分解，年末对规划的执行情况进行评价。

3. 信息安全重要内容规划

1）规划内容：信息安全重点内容（信息安全架构、信息安全专题等）。

2）承担主体：外部机构或内部人员。

3）规划期限：根据实际情况不定期进行。

4）规划要点：根据实际需要，灵活进行。每年对是否需要特定内容规划进行决策，并对规划的执行情况进行评价。

8.2 信息安全建设

8.2.1 信息安全建设原则

1. 以应用为目标，以需求为导向

信息科技的目标是提高银行信息化管理水平，通过加强信息集中，提高对重大事项决策的科学性和时效性，从而提高整个银行的决策和管理水平。信息安全的重要任务是保障业务应用系统的稳定可靠运行。

2. 统一标准、统一规划、统一建设、统一管理

信息安全建设是一个复杂的系统工程，涉及面广，需求复杂。为了保证安全建设能够顺利进行，需要制定统一的技术标准和管理标准体系，进行统一的规划、建设和管理，从整体上保证银行业务的安全性和可用性。

3. 满足监管机构信息安全管理政策，适度安全

银行运行者涉及社会安全、国民经济的大量业务应用系统和数据，监管机构对于银行信息安全非常重视。确保这些应用系统和数据的安全是银行持续、稳定发展的保证，因此必须将信息安全保障体系的建设作为银行建设的重要内容对待。同时，在保证安全的前提下，要确保业务应用系统的可用性。当安全机制影响到业务应用时，可以采取适

当的风险处置措施，降低业务应用的风险。

4. 充分利用现有资源，节能减排

充分利用现有的设备资源，充分考虑应用需求进行硬件资源的配置。加强服务资源的整合，引入集中存储、集中运算、虚拟化等技术，提高对基础设施的利用率。降低银行整体能耗，达到节能减排目标。

5. 以点带面，分步实施

将银行信息安全与实际发展需要充分结合，分阶段完成信息安全整体建设。充分评估系统风险，以解决基本风险为安全防护需求，逐步完善银行安全保障体系建设。在保证应用需求的基础上，根据风险需求与应用情况，不断完善银行安全建设，最终建立起全面、可持续发展的银行信息安全保障体系。

8.2.2 信息安全建设依据

（1）基础类标准

1）《电子银行安全评估指引》。
2）《银行业金融机构信息系统安全保障问责方案》。
3）《商业银行信息科技风险管理指引》。
4）《银行业金融机构信息科技外包风险监管指引》。
5）《网上银行系统信息安全通用规范》。
6）《商业银行数据中心监管指引》。
7）《银行业金融机构信息科技非现场监管报表》。
8）《金融行业信息安全等级保护测评服务安全指引》。
9）《金融行业信息系统信息安全等级保护实施指引》。
10）《金融行业信息系统信息安全等级保护测评指南》。
11）《银行业重要信息系统突发事件应急管理规范》。
12）《计算机信息系统安全保护等级划分准则》（GB 17859—1999）。
13）《信息系统安全等级保护基本要求》（GB/T 22239—2008）。

（2）应用类标准

1）《信息系统安全保护等级定级指南》（GB/T 22240—2008）。
2）《信息系统安全等级保护实施指南》（信安字［2007］10 号）。
3）《信息系统通用安全技术要求》（GB/T 20271—2006）。
4）《信息系统等级保护安全设计技术要求》（信安秘字［2009］059）。
5）《信息系统安全管理要求》（GB/T 20269—2006）。
6）《信息系统安全工程管理要求》（GB/T 20282—2006）。
7）《信息系统物理安全技术要求》（GB/T 21052—2007）。
8）《网络基础安全技术要求》（GB/T 20270—2006）。

9）《信息系统安全等级保护体系框架》（GA/T 708—2007）。

10）《信息系统安全等级保护基本模型》）（GA/T 709—2007）。

11）《信息系统安全等级保护基本配置》（GA/T 710—2007）。

（3）其他类标准

1）《信息安全风险评估规范》（GB/T 20984—2007）。

2）《信息安全事件管理指南》（GB/Z 20985—2007）。

3）《信息安全事件分类分级指南》（GB/Z 20986—2007）。

4）《信息系统灾难恢复规范》（GB/T 20988—2007）。

（4）信息安全框架

1）开放系统安全框架（ISO/IEC 10181-1）。

2）鉴别框架（ISO/IEC 10181-2）。

3）访问控制框架（ISO/IEC 10181-3）。

4）抗抵赖框架（ISO/IEC 10181-4）。

5）完整性框架（ISO/IEC 10181-5）。

6）保密性框架（ISO/IEC 10181-6）。

7）安全审计框架（ISO/IEC 10181-7）。

8）管理框架（ISO/IEC 7498-4）。

9）安全保证框架（ISO/IEC WD 15443：1999）。

8.2.3 信息安全建设包含的内容

信息安全建设与信息安全规划息息相关，信息安全建设使得信息安全规划得以落实，因此信息安全建设必须沿着信息安全规划的指引方向前进，而对信息安全建设结果的检验又反过来形成下一轮信息安全规划的输入。信息安全规划包括信息安全战略规划、信息安全体系规划和信息安全重要内容规划。与之相应，信息安全建设有信息安全体系建设和信息安全项目建设两种形式，它们对信息安全管理体系规划和信息安全重要内容规划形成支撑，从而最终对信息安全战略规划起到支撑和落地的作用。需要注意的是，信息安全管理体系规划和信息安全重要内容规划都可能形成具体的项目，因此信息安全项目建设可以对信息安全管理体系规划和信息安全重要内容规划形成支撑。其相互关系见图 8-3。

8.2.4 信息安全管理体系建设

信息安全管理体系的建设根据不同银行自身特点，会有所不同。都需要根据信息安全管理体系的规划，结合国际国内相关标准进行具体的落地实施。信息安全管理体系的建设可参考本文对信息安全管理体系的模块化划分进行。在进行具体信息安全管理体系建设时，特别要注意以下几点。

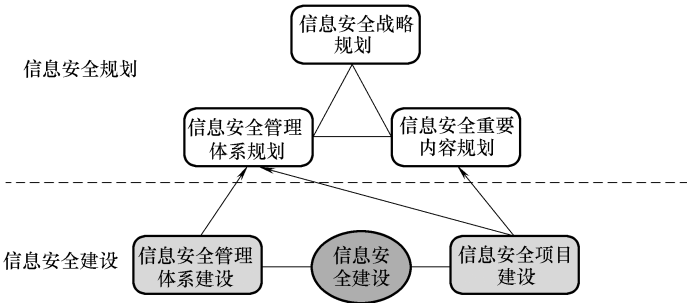


图 8-3　信息安全建设对信息安全规划的支撑

1. 有效融合，固化标准，确保体系的持续改进

信息安全管理体系的落实需要结合国际国内标准特别是银行业相关标准。在应用这些成熟标准过程中，一定要从深层次全局性理解这些标准理念入手，将这些先进理念应用到银行日常管理实践中去，做到与行内原有架构、流程的有机融合，通过标准进行固化；同时在体系运行过程中，要遵循持续改进（PDCA）的理念。结合内外部环境变化、政策要求、业务变革、产品创新等内容，持续开展差距分析、风险评估、有效性测量等工作，不断纠正存在的偏差，才能确保信息安全管理体系的有效运作，逐步提升信息安全整体保障能力。

2. 建立流程，明确要求，强化体系执行效果

信息安全的产生大都源于未严格执行已有的制度和标准，即使再先进的管理体系标准，再完善的制度要求，若不能执行落地都将形同虚设。因此，在体系的建立过程中，要针对与最佳实践的差距分析，结合当前的组织架构，选定符合实际的控制措施，建立职责明确的管理流程，确保其可操作性；在体系建立之后，还要强化制度的执行，加大监督检查力度和责任追究，通过持续教育培训引导员工从被动的风险应对变为积极主动的风险防范；同时，还应建立完善信息安全事件管理机制，及时报告、响应、跟踪、分析各类信息安全风险事件，最大限度地降低信息安全风险带来的损失。

3. 自上而下，全员参与，建立信息安全文化

信息安全涉及各个条线、各个岗位、各个业务流程。在建立信息安全管理体系过程中，首先要开展顶层设计，明确保护的对象、安全等级分类、差异化安全保护策略等。进而明确各部门及员工的职责，采用自上而下的推进方法，组织和动员全体员工共同参与该项工作。尤其是在资产识别和风险评估阶段，更离不开全体员工的努力。通过有效的教育和培训，逐步建立和发展信息安全管理文化，提高和强化员工的信息保护护的意识与能力。

8.2.5　信息安全项目建设

信息安全规划的结果，往往会形成一些具体的项目以支撑规划的落实，包括单独的

信息安全项目及在进行其他信息技术项目时对信息安全的落实（图 8-4）。

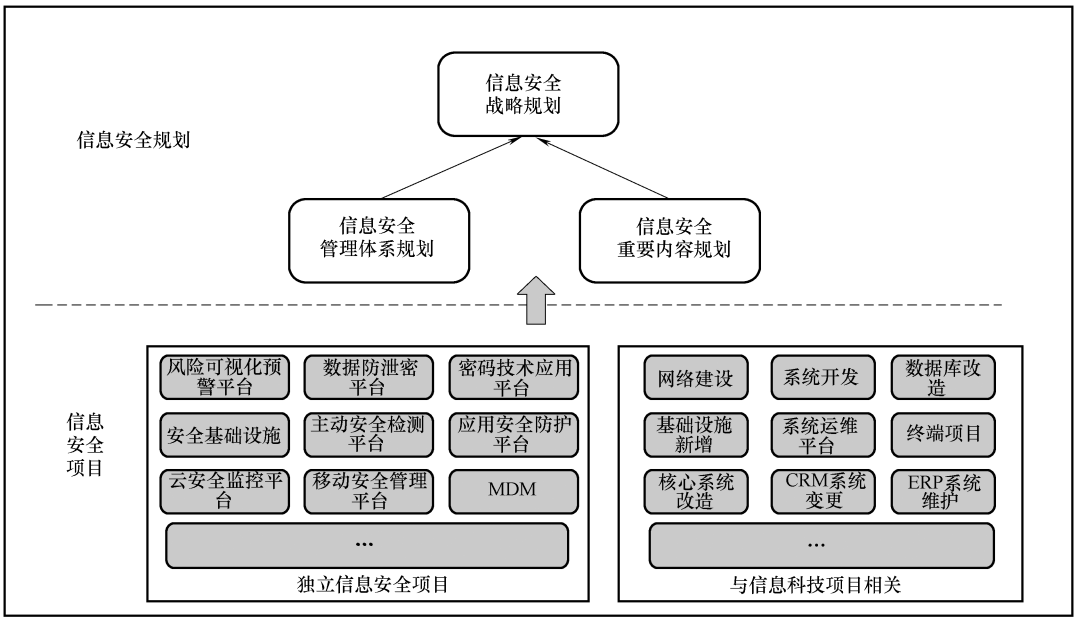


图 8-4　信息安全建设对信息安全规划的支撑

不管是哪种情形，都可以基于信息技术项目的生命周期对信息安全项目加以管理。该过程包括信息安全需求分析、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付及安全服务商选择等阶段。

1. 信息安全需求分析

信息技术项目建设初期，在考虑功能需求、性能需求时，还需考虑信息安全需求。虽然不同项目安全需求不尽相同，但都会考虑本项目的一些基本安全需求：身份鉴别、完整性、抗抵赖、机密性、可用性及授权。以下是一个银行应用系统的安全需求。

（1）身份鉴别　需求分析说明书中系统服务面向的用户群体及数量是否明确，用户的分类情况，用户重要性级别是否明确。

（2）完整性　业务是否与行外机构存在数据交互情况，数据的重要性和传输差错率的容忍度是否明确。

（3）抗抵赖　是否明确数据传输过程中会面临哪些情况，导致数据发送方否认发出数据；是否明确数据传输过程中会面临哪些情况，导致数据接收方否认接收到数据。

（4）机密性　是否明确存在什么样的交易数据；传输的数据是否需要加密；数据是否需要加密存储。

（5）可用性　是否需要 7 ×24 提供服务；容错、容量、灾备的情况如何。

（6）授权　是否需要面向互联网提供服务；是否需要面向办公提供服务。

2. 安全方案设计

根据项目的安全保护需求选择基本安全措施，并依据风险分析的结果补充和调整安

全措施，对信息系统的安全建设进行总体设计。根据信息系统实际情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

3. 产品采购和使用

对于信息技术项目建设，通常会进行产品采购和使用，为了确保安全，应注意：

1）确保安全产品采购和使用符合国家的有关规定。

2）确保密码产品采购和使用符合国家密码主管部门的要求。

3）预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

4. 自行软件开发

对于信息技术项目中自行软件开发的情形，需要加强信息安全保障工作，主要包括：

1）应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制。

2）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。

3）应制定代码编写安全规范，要求开发人员参照规范编写代码。

4）应确保提供软件设计的相关文档和使用指南，并由专人负责保管。

5）应确保对程序资源库的修改、更新、发布进行授权和批准。

5. 外包软件开发

对于信息技术项目中自行软件开发的情形，需要加强信息安全保障工作，主要包括：

1）应根据开发需求检测软件质量。

2）应在软件安装之前检测软件包中可能存在的恶意代码。

3）应要求开发单位提供软件设计的相关文档和使用指南。

4）应要求开发单位提供软件源代码，并审查软件中可能存在的后门。

6. 测试验收

为了保证信息技术项目的安全性，客观地了解信息技术项目的安全状况，需要根据信息技术项目实际情况进行安全测试，具体包括：

1）应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告。

2）在测试验收前应根据设计方案或合同要求等制定测试验收方案；在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。

3）应对系统测试验收的控制方法和人员行为准则进行书面规定。

4）应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。

5）应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

7. 系统交付

测试验收通过后，信息技术项目将进入交付运行阶段，此时的安全要求包括：

1）应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。

2）应对负责系统运行维护的技术人员进行相应的技能培训。

3）应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

4）应对系统交付的控制方法和人员行为准则进行书面规定。

5）应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

8.3 案例介绍：某股份制商业银行信息安全规划实例

随着互联网金融和信息化技术的快速发展，我国商业银行在网上银行、电子商务、电子支付工具等新的服务模式上正在发生着深刻的变化。如何进一步提高商业银行信息安全防护的能力和水平，保障其银行业务稳健发展，是信息安全工作面前的迫切任务。为此，某股份制商业银行（以下简称 A 行）制定了 2015—2019 年信息安全规划。

8.3.1 概述

随着信息化技术的不断深入，应用水平的不断提高，A 行对信息安全的要求也将越来越高，如何确保关键和重要信息系统长期稳定运行，如何防止重要信息数据泄漏，如何避免信息安全事件对 A 行声誉风险、操作风险和经营风险造成严重影响，是目前 A 行信息安全工作面临的严峻威胁和挑战。如何进一步提高 A 行信息安全保障能力和水平，保障 A 行业务发展和快速转型，是信息安全工作面前的迫切任务。

为完善 A 行信息安全总体保障框架，促进 A 行信息技术持续健康发展，特制定本规划。

8.3.2 A 行信息安全现状

A 行科技开发部历来高度重视信息安全工作，为了不断应对来自互联网的各种攻击和探测行为，基于纵深防御思想，A 行经多年建设，在安全基础设施建设、系统安全评估、安全加固和信息安全事件预防处置能力等方面逐年加强，各项安全保障措施到位，具体内容包括：

1）对全行网络进行了严格的安全域划分，实现信息资源的访问控制，强化网络安全区域间的访问控制；建立了全行性的网络应用流量监控系统，实现全行集中/分布式的网络层协议安全监控系统。

2）建立了全行性网络入侵防护系统，实时监测、阻断各种异常及攻击行为；建立了全行网络层安全内容审计系统，与运营商签订网络攻击防范专项保障服务，可针对大

流量网络攻击（如 DDoS、CC 等）进行流量清洗。

3）建立了覆盖全行的桌面管理系统和计算机病毒防治系统，支持办公软件、防病毒软件等应用软件的统一部署和升级；实现了全行办公终端与互联网上网终端的安全分离，降低了信息泄露风险。

4）全面实施生产运行和系统开发的精细化安全管理，从需求评审、代码安全、安全测试和渗透测试等多角度建立安全控制体系，特别是在移动互联网安全现状不容乐观的情况下，落实各项安全技术要求，提高抵御移动互联网攻击的防护能力，提升信息安全工作对业务发展的促进作用。

5）推进容灾备份体系建设工作，进一步完善应急响应机制和灾难备份中心建设，特别是完成分行同城灾备系统，年内实现总行灾备系统的全业务覆盖。

6）每年聘请国家级安全测评机构对三级以上的信息系统进行等级保护和风险评估工作，每周对互联网应用系统进行安全漏洞扫描，每季度进行远程渗透测试等工作。

7）在国密算法、量子保密、安全芯片等方向进行研发及改造工作，逐步扩大安全密码体系的应用范围，依托安全芯片的内嵌技术，形成 A 行设备的安全标识体系，大力发展移动终端安全解决方案的应用及推广。

8）逐年完善信息安全管理制度体系，提高制度编制质量，强化制度执行力度，进一步提升信息安全管理标准化、规范化水平。

长期运行实践表明，上述安全防线有效抵御了来自各个方面的威胁和攻击，不仅技术完整性好，而且满足了国家和行业监管部门的各项合规性要求。

8.3.3 A 行当前面临的主要风险

随着信息技术的不断发展，新型网络攻击层出不穷，技术不断翻新，A 行的信息科技系统所面临的安全威胁也更加复杂，并呈现出安全管理的多样化和复杂化趋势。与此同时，国家、央行和监管部门也对信息系统的安全、内控和审计提出了更高的要求，不断增强的业务连续性需求也对网络安全提出了严峻的挑战。A 行信息系统当前面临的主要风险和威胁如下：

1）来自互联网的恶意攻击威胁依然很大。目前，A 行主要的安全威胁依然是来自互联网的恶意网络攻击。网上银行、手机银行更是攻击的重点目标。随着 A 行在移动互联网不断开发新的业务种类，移动作业模式更是带来了新的安全威胁，包括人员管理的风险、数据安全的风险、保护隐私的法律风险、黑客攻击的风险等诸多方面。

2）信息科技服务的外包风险依然存在。除生产系统运维外，A 行大部分信息系统的开发和技术支撑工作通过外包开展，存在一定的外包人员主动或被动泄漏敏感信息的风险。

3）操作风险对信息系统的影响依然较大。A 行新核心系统上线后，系统之间的耦合性变得越发紧密，一个信息系统出现故障可能会引起其他相关模块出现新的问题。随着 A 行新业务系统建设的不断投产，运维人员的增加也会带来一定的操作风险。

A 行通过多年的信息安全建设工作，已经建立了较为完整的信息安全技术体系，形成了注重可操作性的、完整的信息安全防御机制，实行了基于国家政策要求的信息安全等级管理制度，并通过安全基础设施建设和综合性安全技术措施构建了完善的安全技术防护体系。但随着互联网技术的广泛应用，新应用和新技术的大量涌现、软件系统中存在的安全漏洞、网络和应用协议中固有的安全缺陷，以及黑客攻击技术发展和有组织网络入侵活动的日益活跃，都时刻威胁着 A 行信息系统的健康稳定发展。A 行必须主动适应互联网和安全环境变化，准确把握银行业务和信息安全技术发展趋势，有效化解各类信息安全风险，完善信息安全防护体系，大幅提升信息系统抵御风险和防控的能力。

8.3.4 A 行信息安全规划内容

A 行根据实际情况，本着以安全保发展、以发展促安全的指导思想，需进一步加强信息安全工作的统筹规划能力，进一步明确信息安全工作的责任和关系，逐步建立起技术、管理和运营等多层次的信息安全技术体系，完善策略、制度、规范等安全要素，适度安全，注重实效，合理推进信息安全管理体系建设。

1. 信息安全总体规划设计原则

为落实好信息安全保障工作，A 行信息安全的总体规划及建设将遵循以下原则：

1）统筹规划，联动协调。从全行信息安全保障的总体高度出发，系统规划和建设 A 行信息安全技术体系，同时明确各部门、各分行等相关单位的安全责任，加强横向沟通和协调，指导全行建立联动协调的安全防范和响应机制。

2）资源共享，注重实效。要从 A 行信息安全的实际情况出发，综合平衡安全成本与风险，优化信息安全资源配置，适度安全，注重实效，合理进行信息安全体系建设。

3）分级保护，突出重点。落实信息安全等级保护国策，大力推进信息安全等级保护建设；根据信息系统应用业务的重要程度及实际安全需求，实行分级、分类、分阶段保护；加强对 A 行重要信息系统的日常检查力度，保障信息安全和系统安全正常运行，维护国家金融安全。

4）广泛参与，齐管共建。信息安全是一项全员参与的系统工程，通过各种手段宣传和普及信息安全意识及常识，广泛组织和动员全行共同参与信息安全技术体系建设工作。

2. 信息安全规划总体目标

本次信息安全规划的总体目标是：形成与 A 行信息化发展规划相配套、与业务发展目标相适应的信息安全管理体系，保障 A 行软件开发、生产运行、网络建设全生命周期的信息安全，确保各类信息安全技术机制与措施健全和完善，全行信息安全意识和基本防范能力进一步提高，为 A 行信息科技稳定发展提供有效的信息安全技术。

3. 信息安全规划蓝图

为确保本次信息安全规划总体目标的顺利达成，特拟定了 A 行分阶段的发展蓝图：

1）2015—2016 年为信息安全技术体系全面建立阶段。在这一年当中，A 行将完成各项信息安全基础设施和平台化建设工作，同时各分行的信息安全技术体系建设也基本到位，初步形成具有主动防御能力的信息安全技术体系。

2）2017—2018 年为信息安全管理体系整合阶段。在这一年当中，A 行将对前一阶段完成的信息安全基础做进一步修改和完善，通过各项信息安全运营机制和管理制度，提高信息安全的整体防御能力，全面建成较为完善的信息安全管理体系。

3）2019 年为 A 行信息安全持续改进阶段。通过上述两阶段的建设工作，确保 A 行所有信息系统应全面达到整体安全防护要求，服务好 A 行各项信息科技发展的需求，为实现业务发展战略提供坚实的信息安全技术支撑和管理控制，为信息安全下一次规划打好坚实基础。

4. 信息安全典型系统规划

为实现 A 行信息安全总体目标，确保信息安全任务得以落实，A 行在 2015—2019 年期间的信息安全建设包括了下述主要信息安全系统和体系的建设。

1）风险可视化预警平台。安全管理最大的问题是不知道问题在哪里，何处不安全，以及对安全事件演变的趋势判断。风险可视化预警平台的建设目标就是通过对大量业务系统、安全设备、网络设备所产生的海量数据进行采集和分析，以及根据历史发生事件的数据挖掘和趋势判断，从各种单一的安全事件向统一的关联分析过渡，实现面向业务的安全监控，主动发现网络和操作异常行为，加强应急措施和应对能力，及时阻止各类违规行为的发生，综合研判信息安全事件所产生的影响，并为 A 行战略规划和战略决策提供必要的依据及参考。

通过风险可视化预警平台的建设，有效覆盖总行和 30 多家分行的生产网络、办公网络和互联网络区域，对 A 行现有网络中部署的网络设备（如路由器、交换机）、安全设备（防火墙、IDS、漏洞扫描）、业务服务器等所有设备产生的日志进行统一的采集和甄别，以及对全网数据流和网络行为的过滤和分析，并通过可定义的事件对象和类型，将所有设备产生的安全事件加以关联分析，最终得出当前信息安全的总体态势。安全人员将这些网络和日志信息组合到一个可重用的和标准化的数据框架，能够获得全面的风险态势感知能力，并迅速而有效地应对各类未知的高级威胁。

2）数据防泄密平台。A 行目前已经建成了较为完善的信息科技系统，如核心业务系统、客户信息管理系统、办公系统、财务系统，这些系统的数据主要集中存储在数据库中。但在实际工作过程中仍有部分资料散落在员工的计算机设备上，有时需要对系统中的数据进行再加工，这些都不可避免的导致在员工的计算机设备上存储敏感数据，安全风险较高，容易出现丢失、泄露、病毒损坏、非法获取等情况。同时，A 行员工也多需要回家处理各类遗留的工作，这也会存在将关键或敏感信息数据泄漏到外部的风险。

为此，A 行数据防泄密平台将采取“隔、审、密”的机制来确保数据全生命周期的安全，本项目所需技术手段包括安全桌面、文档加密及授权管理、文件集中存储管理、计算机硬盘加密四类。在建设数据防泄密安全保护体系的过程中，将从在线数据、在线—离线转化、离线数据三个方面着手建设全流程的数据安全防护体系，建成贯穿数

据产生、存储、传递、使用、销毁全流程的数据安全防护体系。

3）密码技术应用平台。依托新核心系统再造项目，A 行密码技术应用平台已经初具规模，它不仅仅是一个产品或系统的建设，更是一个安全体系和应用安全架构的建设。目前 A 行密码技术应用平台已经初步建成，构建起了安全基础设施平台、用户安全平台及客户安全平台等三大技术支撑平台，目前正在不断完善和优化当中。

其中，安全基础设施平台是基础并支撑后两个平台，包括安全的基础服务、安全设备及密钥服务等；用户安全平台则侧重服务于行内员工为用户的各类应用系统，主要提供对用户的标识管理、认证支撑功能；而客户安全平台则主要服务于银行客户为用户的应用系统，如网络银行系统、电话银行系统等。用户安全平台和客户安全平台具有许多相似性，但主要差别在于服务于不同用户对象。目前客户安全平台已经建成了支持多种安全机制和认证方式的综合认证系统，包括 IC 卡功能支持、OTP 认证支持、PKI 证书认证支持、手机认证码支持、密码认证支持等。其中，IC 卡密钥管理系统、数据准备系统、OTP 密钥管理系统等已经初具规模，后续进行适应性改造，扩展对国有算法（SM2/SM3/SM4）的支持，以及对新型金融支付工具的管理功能，可快速地提供相关安全服务，确保新型金融支付工具的安全性、保证在交易过程中遵循相关安全技术标准和规范。

密码技术是信息安全核心要素，密码技术的应用是一个循序渐进的过程，其建设目标是服务好业务发展、服务好信息安全。A 行一直非常重视国产自主知识产权密码技术的应用，不断推进国产密码算法应用工作和试点示范项目，积极创新新型金融支付工具。

4）安全基础设施。信息安全基础设施具有投资规模大、技术要求高的特点，为达到资源共享、合理投资的目的，信息科技部规划建立和完善包括主动恶意代码检测、防 DDoS 攻击、全局入侵检测及监控、安全事件响应和跟踪在内的全行性信息安全基础防御体系，建立起覆盖全行的信息安全监控和服务网络，提高基于内容安全的监测分析和疏导处置能力，有效控制不良信息的扩散，并通过统一、规范的信息安全基础设施，为风险可视化预警平台提供各类信息安全基础数据单元。

5）移动智能终端安全管理系统。A 行目前开发的基于智能终端的应用已经超过 3 个，应用推广后行内采购的移动设备数量将达到 3000 台左右，软件开发、设备购置和通信的费用总额在 2000 万人民币以上。目前这些设备没有进行有效的设备和应用发布方面的安全管理，手工台账方式不能做到实时性和有效性。通过移动智能终端安全管理系统的建设，能够对 A 自购的移动智能终端设备进行安全管理。

国内移动智能终端服务在迅速发展的同时，原先在 PC 电脑上上演的信息安全问题也在移动终端上再次发生，设备制造商、网络服务商、应用服务提供商和最终客户都已经意识到此问题，并且因为移动智能设备的便利性和时时在线属性，导致其所面临的信息安全风险更为严重。

A 行移动智能终端安全管理系统建成后，将作为全行统一的安全管理平台，对总分行各条线购置的智能设备和开发的移动应用软件进行统一安全策略管理，可以监控到设

备的越狱等不合理使用行为，能够在设备遗失、被盗时远程擦除关键应用和数据，能够实时控制移动设备开展业务的范围，确保 A 行的移动金融业务合规开展，整体提升 A 行对移动智能终端的信息安全管控能力。

6）安全管理体系重检与规划。2008 年 A 行通过信息安全管理体系规划咨询项目，逐渐形成一套较为完整的信息安全管理工作模式，使得信息安全各项工作有序展开。但伴随信息安全技术的发展和 A 行业务发展战略及科技战略的变化，科技工作将围绕全面风险管理、全面质量管理和全面架构管理展开，现有的信息安全管理体系已经不能适应和满足管理变化的要求，同时在信息安全实践工作中，原有体系也逐渐反映出一些体系设计层面的问题。

为应对当前内外部信息安全管理的挑战，进一步提升 A 行信息安全管理能力，信息科技计划启动信息安全管理体系重检与规划项目，重检 A 行现有信息安全管理体系，规划 A 行未来信息安全管理工作蓝图。该项目主要工作内容有：

① 全面重检并完善现有管理体系，规划新战略期的信息安全重点工作。

② 打造全面科技风险管理向下的信息安全管理工作机制。

③ 制定信息安全技术架构视图和架构应用规范。

④ 制定信息安全评审模板和实施流程。

⑤ 对信息安全重点领域，如电子银行安全、数据安全等进行重点规划。

通过上述工作，将逐步建成与 A 行当前业务和科技战略发展要求相适应的信息安全管理体系，为实现 A 行的业务和信息技术的运行提供一个安全稳定的发展环境。

第 9 章
信息安全监控与检查

基于信息安全管理体系 PDCA 的核心理念，信息安全监控与检查作为其中的一个重要环节，对银行是否能够及时识别信息安全风险、实现信息安全工作的持续改进起着至关重要的作用。本章介绍了银行业信息安全监控与检查的主要关注点、开展方式、监控与检查的具体内容，在此基础上，对如何在银行信息安全管理过程中利用监控和检查手段有效识别信息安全风险并针对性地部署管控措施进行了分析。

9.1 信息安全监控与检查概述

信息安全监控是指利用安全技术手段，通过实时监控网络或主机活动，监视分析用户和系统的行为，审计系统配置和漏洞，评估敏感系统和数据的完整性，识别攻击行为，对异常行为进行统计和跟踪，识别违反安全法规的行为，使用诱骗服务器记录黑客行为等功能，使安全管理员有效地监视、控制和评估网络或主机系统。信息安全监控的核心是主动安全管理、积极防御的思路，通过对观察到的现象进行记录，分析产生的异常情况，以判断所应采取的安全措施。

信息安全检查与信息安全监控有机结合，是对信息安全风险、信息安全部署、信息安全的不足和措施的有效性等进行综合检查，从而有效改进信息安全效果与效率的一种工作方式。信息安全检查的方式可以是多种多样的，既可以是由信息安全执行团队自发性的安全检查工作，也可以是由信息安全管理团队发起的系统化的信息安全检查工作。针对不同的信息安全领域所采取的检测检查措施也存在较大的差异性，既可能是安全检测技术的应用，也可能是安全管理措施的部署等，在检查的执行周期上也可以按照银行实际的安全管理需求、安全管理成熟度来进行开展。

信息安全监控与检查不应该是孤立的，与整体的信息安全管理一样，也应该是一个持续管理、持续改进的过程，通过监控与检查过程中及时的识别风险，并在此基础上进行分析、处置，以达到持续改进的目的。

9.2 信息安全监控的开展

1. 信息安全监控分析与处置

如图 9-1 所示，信息安全监控的工作重点是关注威胁与事件，通过信息安全技术手段的应用，关注终端、路由器、交换机、防火墙、安全传输平台、操作系统、数据库、应用系统等层面所面临的威胁和事件，识别与分析其所面临的安全威胁和事件。信息安全的监控需要与后续分析处置环节结合起来，通过与安全事件管理流程、应急响应流程的对接，将安全监控管理切实地落地。

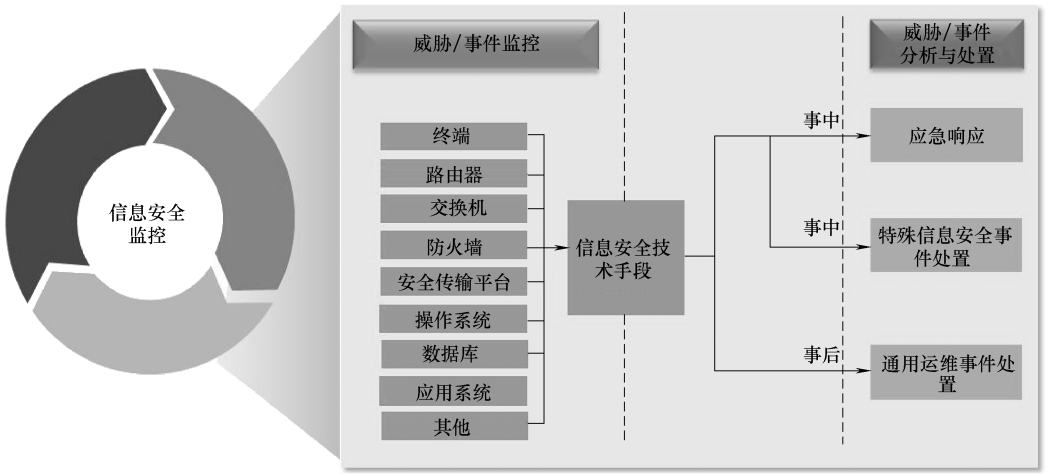


图 9-1 信息安全监控分析与处置

2. 信息安全监控相关的技术手段

信息安全监控技术的发展可以分为单机时代、互联网时代、大数据及云时代。随着信息科技的整体的发展，安全监控技术也随之蓬勃发展，体现为更加高效的威胁及事件的识别、分析效率。

（1）单机时代的典型安全监控技术 该技术包括：

1）病毒码识别技术：计算机节点病毒识别。

2）漏洞识别技术：网络入侵识别。

3）协议分析技术：应用协议分析技术。

4）行为异常分析技术：DDoS 攻击识别。

（2）互联网时代的典型安全监控技术 该技术包括：

1）病毒码识别技术：网关病毒流量识别。

2）漏洞识别技术：WEB 应用攻击识别。

3）行为审计技术：上网行为管理技术、网络行为审计技术、数据库审计技术。

4）信誉评估检测技术：僵尸、钓鱼、垃圾邮件等云识别技术、入侵诱骗分析技术。

（3）大数据及云时代的典型安全监控技术 该技术包括：

1）动态沙盒分析技术：虚拟沙盒分析技术。

2）安全大数据关联分析技术：综合全网安全系统日志或数据包的海量数据关联分析技术、网络流量建模分析技术。

3. 安全日志分析在安全监控中的重要作用

安全日志是安全监控及后续处置的重要输入。目前银行业对安全日志分析的技术应用已经日趋成熟，在市场上也发现有众多的厂家提供安全日志分析的解决方案。具体的关于安全日志分析的技术解决方案将在本书的技术部分与读者进行分享，但是在进行技术应用的同时，还需要通过一系列的安全管理措施来对安全日志的分析过程加以规范与管理，具体的内容如下。

（1）安全日志记录

1）登录验证访问记录：可包括账号异常登录情况、口令猜测情况等。

2）设备配置发生修改记录：可包括办公地址段登录生产和测试网段的网络设备并更改配置、远程 VPN 用户登录网络设备更改配置等。

3）系统管理员和系统操作者的活动：可包括非计划时间内的操作及其他敏感操作等。

4）系统运行错误日志。

（2）安全日志管理

1）需有专门的空间存放日志，关键数据库、操作系统、网络设备及安全设备的日志应尽量进行集中存放，其他系统日志在条件允许的情况下，也要进行集中存放。

2）合理设置日志文件大小，并定期查看日志文件存储的空间是否足够。

3）日志的访问、查看，只能由相关授权人员完成，非授权人员不得拥有对日志的操作权限；日志审阅人员应独立于系统管理员。

4）应用管理员必须经过安全管理部门领导授权同意后才能查看日志。

（3）安全日志分析 安全管理员需熟悉日志的存放位置，具有日志审阅的基本技能，如能解读日志内容，判断违规操作及安全事件等。

（4）安全日志保护

1）日志服务器本身具备抗攻击能力。

2）所有的系统收集过来的日志（包括原始日志）必须保留超过限定的期限。

3）应把备份日志的数据存放在安全区域，防止非授权人员查看、拷贝日志资料。

4）所有系统必须使用统一的系统时间，以确保收集过来的日志是准确的。

9.3 信息安全检查的开展

9.3.1 信息安全检查的组织

鉴于为了保证信息安全检查工作开展的系统性，一般在银行的信息安全管理部门内通过设置明确的专岗负责银行的信息安全检查工作，以保障其有序开展，主要职责包括信息安全检查的规划、组织协调、最终检查结果的沟通确认、检查报告的编制及报告、针对所检查出的安全问题整改措施落实情况的跟踪。另外，在各部门内应配备相应安全员（兼职）以配合信息安全检查工作的开展。安全员负责检查其所辖部门范围内日常安全生产情况，发现问题及时督促整改。

9.3.2 典型信息安全检查的开展方式

信息安全检查的开展方式可以分为各部门自查、信息安全管理部门针对信息安全的例行检查、抽查和专项检查共 4 种。其中信息安全自查工作由各部门所设安全员承担，在工作中接受信息安全管理部门的指导，而其他 3 种方式由信息安全管理部门发起。需要重点提示的是，由于银行业关系到国计民生，其安全运行情况往往相较于其他行业显得更为重要，银行可考虑在重要节假日前夕、重大庆典、重要会议前期、生产系统重大变更前后或根据生产运行需要进行的信息安全专项检查工作。

9.3.3 信息安全检查方式

以主动检测技术，通过评估、检查、测试等方式，全面及时发现银行可能存在的信息安全隐患。典型的信息安全检查的开展形式如下。

1. 风险评估

基于风险评估对银行的生产系统进行综合性安全测试，全面发现系统可能存在的安全隐患，用以评价系统的安全现状并指导安全建设工作的开展。

2. 渗透测试

模拟真实黑客攻击，对银行互联网服务系统进行安全健壮性测试，发现系统存在的安全漏洞和隐患，并配合网站安全监测项目对银行互联网服务系统进行全方位检测。

3. 网站安全监测

对银行互联网服务系统进行实时监测，配合渗透测试项目及时发现系统挂马、被黑及暴露的安全隐患并进行处置。

4. 源代码检查

依据银行应用系统安全开发相关标准、规范、指南对系统源代码进行安全测试。

5. 漏洞扫描

对生产系统服务器进行安全漏洞情况测试，发现服务器、数据库、中间件等可能存在的安全漏洞，验证“漏洞通报”提交漏洞的补丁情况。

6. 安全基线检查

基于银行当前安全基线的配置要求对网络设备、服务器进行检查，识别不符合项并提出整改意见。

7. 漏洞定向通报

针对银行使用的软硬件产品提供最新漏洞信息及其修复措施等，以及时发现并排除信息安全漏洞与隐患，降低信息安全事件发生的可能性，提高信息安全威胁应对与风险管理的能力和水平。

8. 上线前安全测试

在系统上线前进行漏洞扫描、基线检查及安全规范合规性检查。

9. 专项安全检测

针对信息安全的某个特定领域或特定系统进行的专项检测（如手机银行安全测试、弱口令检查等），发现特定领域可能存在的安全漏洞并进行整改，提高该领域的安全防护能力和水平。

9.3.4 信息安全检查内容

1. 典型的信息科技相关安全检查

下文对银行内典型的信息科技相关的信息安全检查内容进行了描述。在具体实践过程中，各银行可按照其自身的信息安全管理信息科技建设的成熟度对安全检查的内容进行相应的调整。

（1）数据中心安全检查 此部分内容可考虑：

1）数据中心及附属设施的建设标准。

2）数据中心的外部供电系统、双 UPS 机组。

3）数据中心内照明、生产、维修用电。

4）数据中心机房环境温度、湿度。

5）数据中心机房场地监控系统、门禁保安系统、紧急联络系统及消防系统等，防静电、防雷、防电磁干扰及防水、防鼠害等技术措施。

6）数据中心各类设备的测试、检修和易损（耗）部件更换。

7）数据中心机房的日常管理情况。

（2）主机设备安全检查 此部分内容可考虑：

1）设备运行监控、维护、故障处理、应急操作规程。

2）主机设备及附属设备的保养及维护工作。

3）设备故障的处理记录。

4）备份设备的可靠性。

（3）操作系统安全检查 此部分内容可考虑：

1）超级用户的管理情况。

2）系统管理员的管理情况。

3）用户的管理情况。

4）系统维护后的记录和归档。

5）系统运行监控、维护、变更、应急操作规程。

6）系统运行故障应急方案。

（4）网络系统安全检查 此部分内容可考虑：

1）重要计算机网络的传输加密、访问控制、身份（设备）验证等安全措施。

2）生产网、测试网和办公网之间的安全控制和隔离措施。

3）与外单位联网的安全控制和隔离措施。

4）与国际互联网（Internet）联网的安全控制和隔离措施。

（5）应用系统安全检查 此部分内容可考虑：

1）应用系统投产前的《测试报告》和《验收报告》。

2）应用系统投产后的运行情况。

3）操作员身份识别管理制度和数据备份制度。

4）应用系统的变更管理。

5）应用系统维护档案的完整性。

2. 银行日常信息科技相关操作

（1）日常操作安全检查 该部分内容可考虑：

1）按规定权限和操作规程操作。

2）密码管理制度执行。

3）日常运行中的异常处理规程和记录。

4）生产运行工作日志。

（2）日常监控安全检查 该部分内容可考虑：

1）主控台信息、系统运行状态和性能、资源使用、网络运行等情况的监控。

2）对系统用户行为的监控。

3）对系统配置的监控。

4）对黑客入侵、病毒扩散等安全事件的监控。

5）对业务交易的监控。

6）应用系统新上线运行和特殊处理日（节假日、结息日、月终、年终决算日等）的运行监控。

（3）生产数据备份安全检查 该部分内容可考虑：

1）日常的备份。

2）特殊处理日的备份。

3）定期整理生产数据的备份。

4）备份介质的存放。

5）定期检查备份数据的有效性。

（4）信息安全开发检查 该部分内容可考虑：

1）开发安全生命周期安全评审情况。

2）源代码访问授权管理情况。

3）开发过程变更管理。

4）上线及系统迁移管理。

（5）技术档案安全检查 该部分内容可考虑：

1）技术档案管理制度和办法。

2）技术档案的完整、准确、安全。

3）技术档案使用登记记录和审批手续。

4）技术档案在保管和传递过程中的保密和安全措施。

（6）终端安全防范检查 该部分内容可考虑：

1）终端层面安全管理工具部署。

2）终端病毒预防和控制。

3）终端黑客防范，入侵事件报告、保护和事件后的检查等。

3. 典型的非科技条线安全检查

（1）信息安全培训检查 该部分内容可考虑：

1）信息安全培训覆盖面。

2）信息安全培训开展评估。

3）信息安全培训效果评价。

4）信息安全培训安全培训记录。

（2）信息安全组织建设情况检查 该部分内容可考虑信息安全组织岗位人员配备及信息安全组织职责履行。

（3）人员安全管理检查 该部分内容可考虑入职过程安全管理、在岗人员安全管理及离职过程安全管理。

（4）外包安全管理检查 该部分内容可考虑外包供应商管理及外包人员安全管理。

（5）信息安全制度建设情况检查 该部分内容可考虑信息安全制度的定期更新。

（6）安全事件管理检查 该部分内容可考虑重大安全事件的报告情况及重大安全事件的处置与记录。

（7）信息安全应急管理检查 该部分内容包括应急方案建设和应急演练情况。

第 10 章
信息安全事件管理

我国银行业在信息安全上虽然取得了长足的进步，但也面临着诸多信息安全事件的困扰。因此银行业对于信息安全事件的有效管理至关重要。本章描述了信息安全事件管理的基本概念、信息安全事件的分类分级、信息安全事件的管理过程，以及银行业信息安全事件的应急处理。

10.1 信息安全事件管理概述

安全事件是指针对业务平台系统，由于硬件、软件、数据等信息资产因非法攻击或病毒入侵等内、外部威胁而遭到破坏、更改、泄漏，最终造成业务平台系统信息安全受到威胁，不能正常运行，从而影响正常的业务发展。作为金融行业的组织整体信息安全战略的一个关键部分，采用一种结构严谨、计划周全的方法来进行信息安全事件的管理是至关重要的。信息安全事件的管理目标旨在确保：

1）信息安全事件可以被发现并得到有效处理。

2）对已确定的信息安全事件进行评估，并以最恰当和最有效的方式做出响应。

3）及时总结信息安全事件及其管理的经验教训。这将增加预防将来信息安全事件发生的机会，改进信息安全防护措施的实施和使用，同时全面改进信息安全事件管理方案。

10.2 信息安全事件分类

信息安全事件可以是故意、过失或非人为原因引起的，根据《信息安全技术信息安全事件分类分级指南》（GB/Z 20986—2007），信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信

息安全事件共7个基本分类，每个基本分类分别包括若干个子类。银行业大多参考该标准制订符合自身实际的信息安全事件分类。

10.2.1 有害程序事件

有害程序是指插入到信息系统中的一段程序，会危害系统中数据、应用程序或操作系统的保密性、完整性或可用性，或影响信息系统的正常运行。有害程序事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件，包括计算机病毒事件、蠕虫事件、木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其他有害程序事件共7个第二层分类。

10.2.2 网络攻击事件

网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。网络攻击事件包括拒绝服务攻击事件、后门攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件共6个第二层分类。

10.2.3 信息破坏事件

信息破坏事件是指通过网络或其他技术手段，造成信息系统中信息被篡改、假冒、泄露、窃取等而导致的信息安全事件。它包括信息篡战事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其他信息破坏事件共6个第二层分类。

10.2.4 信息内容安全事件

信息内容安全事件是指利用信息网络发布或传播危害国家安全、社会稳定和公共利益的内容的安全事件，包括违反宪法和法律、行政法规的信息安全事件；针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件；组织串连、煽动集会游行的信息安全事件；其他信息内容安全事件共4个第二层分类。

10.2.5 设备设施故障

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为使用非技术手段有意或无意的造成信息系统破坏而导致的信息安全事件。设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施

故障共 4 个第二层分类。

10.2.6 灾害性事件

灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。它包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

10.2.7 其他信息安全事件

其他信息安全事件类别是指不能归为以上 6 个基本分类的信息安全事件。

10.3 信息安全事件的分级

根据《信息安全技术信息安全事件分类分级指南》（GB/Z 20986—2007），对信息安全事件的分级可参考 3 个要素，即信息系统的重要程度、系统损失和社会影响。

1）信息系统的重要程度：信息系统的重要程度主要考虑信息系统所承载的业务对国家安全、经济坚实、社会生活的重要性，以及业务对信息系统的依赖程度，划分为特别重要的信息系统、重要信息系统和一般信息系统。

2）系统损失：系统损失是指由于信息安全事件对信息系统的软硬件、功能及数据的破坏，导致业务中断，从而给银行和国家所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价。

3）社会影响：社会影响是指信息安全事件对社会所造成影响的范围和程度，其大小要考虑国家安全、社会秩序、经济建设和公众利益等方面的影响。

根据业务平台系统突发事件的紧急程度和发展趋势，以及对服务的用户造成的影响程度（范围和持续时间），将安全事件分为特别重大事件、重大事件、较大事件和一般事件共 4 个等级。

10.3.1 特别重大事件（Ⅰ级）

特别重大事件是指能够导致特别严重影响或破坏的信息安全事件，会使特别重要的信息系统遭受特别重大的系统损失，即造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于银行是不可承受的。它所产生的社会影响会波及一个或多个省市的大部分地区，极大威胁国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者严重损害公众利益。

10.3.2 重大事件（Ⅱ级）

重大事件是指能够导致严重影响或破坏的信息安全事件，会使特别重要的信息系统遭受重大的损失，即造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，对于银行是可承受的；或使重要信息系统遭受特别重大的系统损失。它所产生的社会影响波及一个或多个地市的大部分地区，威胁到国家安全，引起社会恐慌，对经济建设有重大的负面影响，或者损害到公众利益。

10.3.3 较大事件（Ⅲ级）

较大事件是指能够导致较严重影响或破坏的信息安全事件，会使特别重要的信息系统遭受较大的系统损失，即造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于银行是完全可以承受的；或使重要信息系统遭受重大的系统损失、一般信息系统遭受特别重大的系统损失。它所产生的社会影响波及一个或多个地市的部分地区，可能影响到国家安全，扰乱社会秩序，对经济建设有一定的负面影响，或者影响到公众利益。

10.3.4 一般事件（Ⅳ级）

一般事件是指能够导致较小影响或破坏的信息安全事件，会使特别重要的信息系统遭受较小的系统损失，即造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小；或使重要信息系统遭受较大的系统损失、一般信息系统遭受重大的系统损失。它所产生的社会影响波及一个地市的部分地区，对国家安全、社会秩序、经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益会造成损害。

10.4 银行业突发事件分级管理

2011 年，为规范银行业重要信息系统的突发事件应急管理，提高应对突发事件的综合管理水平和应急处置能力，有效防范银行业信息系统风险。银监会根据《中华人民共和国银行业监督管理法》《中华人民共和国突发事件应对法》及相关法律法规，制定并下发了《银行业重要信息系统突发事件应急管理规范》。

该规范所面向的对象是在我境内设立的政策性银行、国有商业银行、股份制商业银行、邮政储蓄银行、城市商业银行、农村商业银行、农村合作银行、农村信用社、城市信用社，外商独资银行、中外合资银行和外国银行分行。规范中对银行业重要信息系统突发事件应对工作原则、信息系统范围进行了清晰的定义，明确了银监会和银行业金融机构的组织机构及相关职责。银行业由于信息安全事件所导致的突发事件分级将遵从该规范。

该规范中明确规定，银行业金融机构对突发事件依照其影响范围及持续时间等因素进行分级。其分级原则为当突发事件同时满足多个级别的定级条件时，按最高级别确定突发事件等级。规范中将突发事件定义为三级：特别重大突发事件（Ⅰ级）、重大突发事件（Ⅱ级）和较大突发事件（Ⅲ级）。

10.4.1 特别重大突发事件（Ⅰ级）

1）银行业金融机构由于重要信息系统服务中断或重要数据损毁、丢失、泄露，造成经济秩序混乱或重大经济损失、影响金融稳定的，或对公众利益造成特别严重损害的突发事件。

2）由于重要信息系统服务异常，在业务服务时段导致银行业金融机构两个（含）以上省（自治区、直辖市）业务无法正常开展达 3 小时（含）以上，或一个省（自治区、直辖市）业务无法正常开展达 6 小时（含）以上的突发事件。

3）业务服务时段以外，重要信息系统出现的故障或事件救治未果，可能产生上述 1 ~2 类的突发事件。

10.4.2 重大突发事件（Ⅱ级）

1）银行业金融机构由于重要信息系统服务中断或重要数据损毁、丢失、泄露，对银行或客户利益造成严重损害的突发事件。

2）由于重要信息系统服务异常，在业务服务时段导致银行金融机构两个（含）以上省（自治区、直辖市）业务无法正常开展达半小时（含）以上，或一个省（自治区、直辖市）业务无法正常开展达 3 小时（含）以上的突发事件。

3）业务服务时段以外，出现的重要信息系统故障或事件救治未果，可能产生上述 1 ~2 类的突发事件。

10.4.3 较大突发事件（Ⅲ级）

1）银行业金融机构由于重要信息系统服务中断或重要数据损毁、丢失、泄露，对银行或客户利益造成较大损害的突发事件。

2）由于重要信息系统服务异常，在业务服务时段导致一个省（自治区、直辖市）

业务无法正常开展达半小时（含）以上的突发事件。

3）业务服务时段以外，出现的重要信息系统故障或事件救治未果，可能产生上述1～2类的突发事件。

重要信息系统突发事件发生后，银行业金融机构应依据事件影响范围和影响时间的变化，按照上述定义进行事件级别升级。

10.5 信息安全事件管理的过程

信息安全事件管理由4个不同的过程组成，即规划和准备（Plan and Prepare）、使用（Use）、评审（Review）、改进（Improve）。

1. 规划和准备

有效的信息安全事件管理需要适当的规划和准备。为使信息安全事件的响应有效，下列措施是必要的：

1）制定信息安全事件管理策略并使其成为文件，获得所有关键利益相关人，尤其是高级管理层对策略的可视化承诺。

2）制定信息安全事件管理方案并使其全部成为文件，用以支持信息安全事件管理策略；用于发现、报告、评估和响应信息安全事件的表单、规程和支持工具，以及事件严重性衡量尺度的细节。

3）更新所有层面的信息安全和风险管理策略。全银行范围的，以及针对每个系统、服务和网络的信息安全和风险管理策略，均应根据信息安全事件管理方案进行更新。

4）确定一个适当的信息安全事件管理的组织结构，即信息安全事件响应组，给那些可调用的、能够对所有已知的信息安全事件类型做出充分响应的人员指派明确的角色和责任。在银行中，应急响应团队可以是一个虚拟小组，即由一名高级管理人员领导的、得到各类特定主题专业人员支持的小组。例如，在处理恶意代码攻击时，根据相关事件类型召集相关的专业人员。

5）通过简报和/或其他机制使所有的员工了解信息安全事件管理方案、方案能带来哪些益处，以及如何报告信息安全事态。应该对管理信息安全事件管理方案的负责人员、判断信息安全事态是否为事件的决策者，以及参与事件调查的人员进行适当培训。

6）全面测试信息安全事件管理方案。在进行信息安全事件的规划时，应该制订规范的信息安全事件记录单，以便对信息安全事件进行有效记录（表10-1）。

2. 使用

下列过程是使用信息安全事件管理方案的必要过程：

1）发现和报告所发生的信息安全事态（人为或自动方式）。

表 10-1　信息安全事件记录单

信息安全事件记录单				
系统名称		故障编号		
设备名称		设备 IP		
事件信息				
事件类型	系统□　软件■　网络□　终端□　环境设备系统□　应用系统□　安全□　其他□			
事件优先级	1□　2□　3□　4□　5■		事件处理人	
事件报修人			联系电话	
受理日期			受理时间	
结束日期			结束时间	
事件描述				
事件初步处理				
事件初步处理的过程描述,需要记录的详细步骤：				
后续处理过程				
结束日期			结束时间	
事件原因确定,需要明确说明：				
事件处理的方法或者暂时解决途径：				
其他附件(可选)：				
后续建议				

2）收集与信息安全事态相关的信息，通过评估这些信息确定哪些事态应归类为信息安全事件。

3）对信息安全事件做出响应。

① 立刻、实时或接近实时。

② 如果信息安全事件在控制之下，按要求在相对缓和的时间内采取行动。

③ 如果信息安全事件不在控制之下，发起“危机求助”行动（如召唤消防队/部门或者启动业务连续性计划）。

④ 将信息安全事件及任何相关的细节传达给内部和外部人员和/或组织（其中可能

包括按要求上报以便进一步评估和/或决定)。

⑤ 进行法律取证分析。

⑥ 正确记录所有行动和决定以备进一步分析之用。

⑦ 结束对已经解决事件的处理。

3. 评审

在信息安全事件已经解决或结束后，进行以下评审活动是必要的：

1）按要求进行进一步法律取证分析。

2）总结信息安全事件中的经验教训。

3）作为从一次或多次信息安全事件中吸取经验教训的结果，确定在信息安全防护措施实施方面的改进。

4）作为从信息安全事件管理方案质量保证评审（如根据对过程、规程、报告单和/或组织结构所做的评审）中吸取经验教训的结果，确定对整个信息安全事件管理方案的改进。

4. 改进

安全事件管理过程虽然可以反复实施，但随着时间的推移，有许多信息安全要素需要经常改进。这些需要改进的地方应该根据对信息安全事件数据、事件响应及一段时间以来的发展趋势所做评审的基础上提出。其中包括：

1）修订银行现有的信息安全风险分析和管理评审结果。

2）改进信息安全事件管理方案及其相关文档。

3）启动安全的改进，可能包括新的和/或经过更新的信息安全防护措施的实施。

10.6 信息安全事件应急处理

应急处理是指在计算机系统或网络上的威胁安全的事件发生后采取的措施和行动。这些措施和行动通常是用来减小和阻止事件带来的负面影响和坏的后果。

信息安全事件应急处理的目的是限制攻击的范围，同时也限制了潜在的损失和破坏。在事件确认后，无论谁来处理事件，都应该考虑事件处理的合理方式，并确定一个最佳的方式。非常重要的一点是，永远都不要轻视抑制措施，因此太多的安全事件就是忽略了这一点而导致迅速地失控。

银行信息安全应急处理工作需要注意下述方面的内容。

1. 应急处理原则

对于发现信息安全事件的是第一个注意到安全入侵和需要研究的异常现象的人员，或者第三方人员可能会试图根除这些异常或是事件（更常见的是觉察到异常，但最后证明不是安全事件），但由于缺乏专业性，他们经常带来很多麻烦，有可能对系统和文件造成的破坏比攻击者还要严重。因而，这些工作应该由专业的应急响应团队来完成。

一般人员遇到异常情况，遵守以下这些行为规范：

1）在没有向专家咨询之前不要关闭自己的系统或者断开网络。

2）按照银行的报告程序（应急响应策略）向安全负责人报告任何可疑现象。

3）继续监控并记录可疑的现象，直到处理该类安全事件的人员到达。

4）不要修改系统或应用软件。

5）除非得到管理层同意，不要告诉媒体任何信息。

2. 确定适当的响应方式

这一阶段，应急响应团队在明确了事件的发生及掌握相关的信息后，应当选择适当的响应方式。这些选择包括恢复运行、在线响应与离线响应、媒体公关、识别攻击者、起诉和惩罚等。除了这些简单的方式，当然还有其他的。响应的方式不可生搬硬套，只能因地制宜。

（1）恢复运行 最快最简单的响应方式以恢复正常运行为唯一目的。不必过分小心谨慎地进行保护证据、确定责任人、追踪攻击者等一些复杂的工作。相反，其唯一目标在于使被侵袭的系统恢复到正常运行的状态。

这是网站被涂改和拒绝服务攻击突发事件的常见响应。这种响应不需要庞大的计算机应急响应小组或耗费大量精力进行事件调查取证。使用该响应方式的典型方法，一般是用备份来恢复受害系统，然后重新配置防火墙和路由器以防止同类攻击的再次发生。

（2）执行在线或离线响应 响应的基本决策之一是该系统是否可以移出网络。如果该系统是某种不具有备份的硬件解决方案，并且对运行非常关键，那么可能需要在保持系统在线状态下执行响应，这可能导致证据收集和司法鉴定更加困难。

另一方面，为了获得足够证据以识别攻击者，可能需要计算机保持工作状态和在线状态，以监视攻击者的活动并跟踪其来源。由于系统是否可以进入离线状态常常是关系到停止服务的商业问题，因而可能要有非应急响应团队的成员来裁决，这通常是管理层的工作，但在其做出决定前必须让决策者明白各种决定对应急响应的副作用。

（3）媒体公关 公众是否知道该突发事件？公众对此是否有所察觉？如果两个问题的答案均为“是”，那么应当将应急方式中包括对媒体进行攻关，即向新闻媒体适当地公开一些信息。

大多数银行具有公关部门，通过向媒体发布一些与事件相关的有利于银行的信息，能够起到稳定人心、引导公众意识的作用。作为应急响应队伍的领导人应该明白在何种状态下都要使公关人员参与进来，并且使他们成为应急响应团队中不可分割的一部分。“准备”阶段应该使这些人在突发事件发生前有所准备。

（4）识别攻击者 响应策略的目标是否识别攻击者？如果是，那么该响应将需要仔细而且很可能冗长的调查。如果攻击者来自内部，则无须使用外部法律力量即可实现该目标；如果攻击者来自于互联网，那么调查必须借助外部法律力量。如果没有第三方对攻击源进行调查，那么可能永远无法确定攻击者身份，而只能确定攻击的最后一个中继站。此外，任何试图识别攻击者的调查都可能需要大量的时间和资源。

对于正在进行的网络攻击，可能要求采取被动监视，并且可能需要所有受危及系统

保持易受攻击的在线状态，以免打草惊蛇。现在并不是任何一个公司都具备用以识别攻击者的资源，因而只好满足于保护和恢复被侵袭的系统。

（5）起诉和惩戒 是否希望起诉或采取惩戒？如果是，自然需要首先识别攻击者。然后需要以收集和保存的证据来起诉攻击者。这里要注意的是，收集的证据的方式及证据本身必须是司法机关认可的。

3. 可采用的抑制动作

一种响应方式是由一系列的单个或多个动作来组成的。

1）完全关闭所有系统（一种彻底的强力措施，但有时也是明智的决定），能及时地防止进一步的破坏。

2）拔掉网线，从网络上断开。

3）修改所布防火墙和路由器的过滤规则，拒绝来自发起攻击的嫌疑主机的所有流。

4）封闭或删除被攻破的登录账号。

5）提高系统、服务和网络行为的监控级别。

6）设置诱饵服务器作为陷阱。

7）关闭服务。

8）反击攻击者的系统。

事件抑制的一个基本部分是找到攻击者可能安装在系统中的恶意程序和后门程序，这些程序使得攻击者可以不经授权便能重新进入被攻破的主机和网络设备。如果已经安装了后门，删除它们通常是必不可少的操作。可能会有些例外，比如应急响应工作涉及收集法律起诉工作所需要的证据。类似的，如果有人未经授权或得了超级用户的访问权限，或者得到了口令文件的一个拷贝，通常也要尽快地认真更改所有的口令（因为攻击者可能已经破解了其他的口令）。

4. 其他考虑

1）坚持充分定义的和详细的抑制措施。

2）继续用细致有效的手段记录事件期间发生的所有事情、已经完成的事情、花费的时间及其他重要的细节。

3）在事件发生前定义可接受的风险程度。

4）如果有持续性的破坏、如果数据被破坏等，应告诉用户被攻击系统的当前状况。

5）向合适的组织和人报告任何重要的最新信息。

10.7 案例介绍：某商业银行信息安全事件管理办法

第一章 总 则

第一条 为了防止突发事件对某商业银行股份有限公司（以下简称“本行”）的信

息资产造成机密性、完整性、可用性方面的危害，从而给本行带来任何负面影响，特制定本办法。

第二条 本办法旨在加强信息技术人员的责任感，最大程度地防范技术事件，减少因突发事件造成的损失，保障本行各项业务的顺利进行。

第三条 信息安全事件处理应依据“先处置，后责任”的原则。

第四条 本办法适用于本行各级机构和全体员工、承包方人员和第三方人员。

第二章 信息安全事件定义与分类分级

第六条 信息安全事件是指由于自然的或人为的、软硬件本身缺陷或故障等原因，能够对本行信息资产的机密性、完整性、可用性造成危害的事件。信息安全事件包括但不限于在计算机系统或网络系统中发生的对社会、本行造成负面影响的事件。

第七条 根据信息安全事件发生的原因、表现形式等，把信息安全事件分为恶意程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、系统故障事件、灾害性事件和其他信息安全事件七个基本大类。

第八条 根据信息安全事件的影响范围与程度，对其严重程度从高到低分为Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）和Ⅳ级（一般）四个等级。

第三章 组织与职责

第十条 科技信息部成立信息科技应急处置小组，主要职责为：

一、负责信息安全事件的处置工作及事件后续工作，包括事件分析、总结、事件定性及责任认定。

二、如信息安全事件达到业务连续性计划启动条件，配合业务连续性应急处置工作小组处置。

第十二条 将达到业务连续性计划启动条件的信息安全事件纳入业务连续性管理，由业务连续性应急处置工作小组具体负责处置工作。

第四章 管 理 办 法

第一节 事件报告和处理程序

第十三条 信息安全事件报告程序需根据事件级别按对应的报告和处理程序进行处理。

第十四条 所有本行员工或者外包人员，应尽快地报告所发现的信息安全事件。如果发现事件或故障，应立即记录下所有重要的细节，并立即报告给科技信息部的相关系统的负责人员。

第十五条 相关系统的负责人员报告其中心主管，由中心主管根据事件的性质和影

响范围与程度等因素向信息科技应急处置领导小组汇报，信息科技应急处置领导小组组织进行必要的应急措施，对事件进行控制，防止事态进一步扩大。

第十六条 信息科技应急处置领导小组应对信息安全事件判断，如事件发展达到业务连续性计划启动条件的，则第一时间向业务连续性应急处置工作小组报告，由业务连续性应急处置工作小组全面接管应急工作。

第十七条 事件处置程序须包括适当的反馈过程，以确保在信息安全事件处理完成后，能够将处理结果，通知给事件报告人。

第二节 分析与总结

第十八条 当发生信息安全事件时，信息科技应急处置领导小组应及时组织人员进行事件评估、事件处置、事件调查，提交书面的调查报告，必要时可组织有关专家进行鉴定，确定事件原因和责任。

第十九条 信息安全管理领导小组应根据事件处理报告的结果，督促完成如下工作：

一、评估应急计划是否完善，检查应急措施执行落实情况。

二、核实故障损失，会同相关部门对故障后果进行评估。

三、检讨故障处理过程中存在的技术问题、管理及协调问题。

四、形成信息系统故障处理总结报告，必要时提出整改计划和整改时间表。

五、将故障处理报告、故障总结报告等内容定期发布，供全体员工学习交流。

六、防止类似情况重复发生。

第二十条 事件责任单位或部门应按照整改时间表落实整改，并对整改后的情况进行追踪监测。

第三节 事件定性及责任认定

第二十一条 信息安全管理领导小组负责事件处理完毕后事件认定工作。发生信息安全事件后，应组织科技信息部、受事件影响的业务部门、风险管理部组成事件认定工作组，必要时可要求系统开发商或其他合作单位参与。

第二十二条 信息安全事件的责任界定流程如下：

一、事件认定应当进行必要的取证。

二、因软硬件故障引发的事件，应会同供应商共同调查，界定责任。

三、因通信线路故障导致的事件，应会同电信运营商共同调查，界定责任。

四、因人员操作失误导致的事件，应会同科技信息部及事件发生部门的有关人员调查，界定责任。

第二十三条 下列情况事件当事人可以免责：

一、因不可抗力引发的技术事件。

二、因软硬件故障导致的技术事件，经技术专家论证，确认信息系统建设和管理符合相关要求，确属小概率或偶发性事件。

三、因外方原因导致的交易中断。

四、其他经事件认定工作组确认可以免责的情况。

第四节　安全弱点报告

第二十四条　对于观察到的或有怀疑的信息安全弱点，本行员工或外部人员应及时报告给科技信息部相关人员，经科技信息部负责人批准后，由相关的技术人员进行处置，重大问题处理须报信息安全管理领导小组审批，并做好登记备案工作。

第二十五条　信息科技应急处置领导小组负责跟踪已备案的信息安全弱点处置情况。

第二十六条　未经授权，任何人禁止利用任何方法去证明被怀疑的信息安全弱点。

第四章　附　　则

第二十七条　本办法由本行负责制定、解释和修改。

第二十八条　本办法自发布之日起施行。

第 11 章
业务连续性与灾难恢复管理

随着技术的不断发展，银行业的竞争也愈发激烈。银行越来越依赖于计算机系统，因为这里保存着维系生存、参与竞争的重要资产——各种信息资源。信息科技为银行业提供了广阔的业务发展空间和持续创新能力，同时，也带来了诸多风险，如系统故障、网络故障、电力中断、人为操作失误等。这些风险轻则降低银行的服务水平、阻碍业务的正常运营，重则导致大范围、长时间停业，使银行面临信用危机及不良社会影响。对银行而言，计算机系统失效无疑是一场灾难。本章主要讲述了业务连续性与灾难恢复管理的现状与思考、灾难恢复管理流程及业务连续性与灾难恢复管理在我国商业银行的使用案例。

11.1 业务连续性与灾难恢复概述

现如今，灾难恢复能力已成为评价一家银行安全性的重要指标。当发生区域性灾难时，如果某家银行可以一枝独秀地迅速恢复对外服务，其竞争力必然得到凸显。像类似美国“9.11”灾难事件，银行灾备能力与机制变成首当其冲。同样，当面临非区域性灾难时，如果某家银行无法从个体灾难中迅速恢复业务，即会显露其在灾难体系建设和管理上存在的问题。如何建设好业务连续性与灾难恢复管理体系已经成为各家银行一个重要的课题。

20 世纪 90 年代早期，业务连续性和灾难恢复管理主要定位于信息技术灾难恢复，它主要提供在自然灾难和关键部件故障时通过在备份站点恢复技术资产（如系统、网络和数据）。这时典型的恢复时间目标（Recovery Time Objective，RTO）是指灾难发生后，系统和数据必须恢复到的时间点要求，它代表了当灾难发生时允许丢失的数据量，如恢复应用的预期时间大约是 3 天；典型的恢复点目标（Recovery Point Objective，RPO）是指灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求，它代表了系统恢复的时间，如可接受的交易损失大约是 24 小时。它所应用的主要组织机构是高

度规范的行业（银行等金融服务行业）。

到了 20 世纪 90 年代中期，组织机构开始将其业务连续性和灾难恢复计划加入业务过程保护，同时开始开发恢复计划。此时，整个业务持续性计划和灾难恢复计划的框架仍没有大的改动，RTO 和 RPO 要求也没有什么大的改动。

到了 20 世纪 90 年代后期，为了应对千年虫问题，银行业开始重新组织、评估和投资其业务过程和业务持续性计划。传统的 3 天恢复时间开始变得不能满足需要了，对于那些使命关键的应用，其 RTO 开始减少至小于 24 小时，RPO 通常开始设置为灾难发生点（没有工作或交易损失）。随着互联网和电子商务的发展，银行内部处理系统与外部服务提供商、合作伙伴以及客户相关联度日益加强，对业务持续性产生了更高的要求。RTO 和 RPO 的要求进一步减少至 0（意味着没有宕机时间或 7 ×24 小时业务过程可用性）。此时，随着新的风险的增加，业务恢复计划和灾难恢复计划必须开始处理一些新的领域，如运行维护风险（重要支持网站不可用）、安全风险（如 DoS 攻击）、合作伙伴/外包商不可用等。

现在的业务连续性管理/灾难恢复管理更加强调了对业务的支持。严格地说，业务连续性管理/灾难恢复管理包括一系列管理的概念，如业务连续性计划、业务恢复计划、运行连续性计划、事件响应计划、人员紧急计划、危机沟通计划和灾难恢复计划等。在美国 NIST 800-34 信息技术系统连续性计划指南中给出了相关的定义。

（1）业务连续性计划（Business Continuity Plan，BCP） 业务连续性计划强调在中断发生或发生后维持组织机构的业务功能。业务功能的实例可能是组织机构的工资单过程或客户信息过程。一个业务连续性计划可能用于某个特定的业务过程或用于解决所有的关键业务过程。在业务连续性计划中对信息系统的考虑仅限于他们对业务过程的支持。在某些情况下，业务连线性计划可能不会解决过程的长期恢复和返回至正常操作，而仅仅覆盖了过渡期的业务连续性要求。可以将灾难恢复计划、业务恢复计划和人员紧急计划附在业务连续性操作计划（COOP ）中的相关设定相协调以减少可能的冲突。

（2）业务恢复计划（Business Recovery Plan，BRP） 也称为业务重启计划（ Business Resumption Plan），它是解决在紧急事件发生后的恢复业务过程。同业务连续性计划不同的是，业务恢复计划通常缺少确保整个紧急事件或中断时确保关键过程连续性的流程。业务恢复计划的开发应同灾难恢复计划和业务连续性计划相协调，业务恢复计划可以附在业务连续性计划中。

（3）业务连续性操作计划（Continuity of Operations Plan，COOP） 它强调在备用场所恢复组织机构的（通常是一个总部元素）关键功能并在返回至正常操作前最多执行 30 天的功能。因为运行连续性计划解决的是总部级的问题，它的开发和执行独立于业务连续性计划。COOP 的标准元素包括职权授权描述、继任的顺序、关键记录和数据库。因为 COOP 强调组织机构在备用场所恢复组织机构运行能力，此计划不是必须要求包含信息技术操作。另外，小的并不需要重定位至备用场所的中断也不在运行连续性计划的考虑范围之内。

（4）支持连续性计划/信息技术连续性计划 连续性支持计划是信息技术连续性计划的同义词。因为信息技术连续性计划也可以开发用于每一个主要应用和通用支持系统，在组织机构的业务连续性计划 BCP 中可以维护多个连续性计划。

（5）危机沟通计划（Crisis Communications Plan，CCP） 组织机构应在灾难前准备内部和外部沟通流程，它所开发的危机沟通流程通常用于公众服务。危机沟通计划流程应同所有其他计划进行协调，以确保只有得到批准的描述和声明才能发布给公众。计划流程应包含至业务连续性计划的附录。沟通计划通常指定特定人员作为唯一的向公众解释有关灾难响应情况的授权人员，它可能也包括将状态通报至公众的流程。新闻发布的模板应包含至计划中。

（6）计算机事件响应计划（Cyber Incident Response Plan） 组织机构应建立解决信息技术系统受到网络攻击时的流程。这些流程是用于让安全人员能对恶意计算机事件进行标识、缓解和恢复，如对系统和数据的非授权访问、拒绝服务攻击、对系统硬件或软件的非授权修改（如蠕虫、木马病毒等恶意代码）。此计划可以包含在业务连续性计划的附录中。

（7）灾难恢复计划（Disaster Recovery Plan，DRP） 正如其名字，该计划应用于严重事件，通常是灾难性事件，这种事件将在一段较长时间内阻止对正常设施的访问。通常，灾难恢复计划指的是发生紧急事件后，在备用场所恢复目标系统、应用或计算机设施的以信息技术为核心的计划。灾难恢复计划会同信息技术连续性计划有所交叠，但是灾难恢复计划的范围更窄，并且不讨论那些不需要重定位的小中断。

（8）人员紧急计划（Occupant Emergency Plan，OEP） 该计划是为某一个特定设施内的人员制定相应的响应流程，以应对人员、环境或财产的健康和安全产生危害的事件。这些事件可能包括火灾、犯罪攻击或医学紧急事件。人员紧急计划是设施级，特定于地理位置和建筑的结构化设计。

11.2 我国银行业务连续性/灾难恢复管理的现状与思考

经济全球化和金融市场的开放加速，加剧了国内外银行业的竞争格局，金融危机的洗礼使得国际、国内经济和金融环境变得愈加复杂，如何在日趋激烈的市场竞争中实现银行业金融机构的持续发展，如何在愈加恶劣的生存环境和更为复杂的技术应用条件下，增强金融机构应对灾难及突发事件的能力，保障业务连续性运营，成为国内银行业金融机构面临的重点和难点问题。

简单来讲，业务连续性是指在中断或灾难发生时仍然保持服务的能力，无论是由网络连接、服务器中断，还是应用程序瘫痪所导致的中断。对银行和金融机构而言，原则上，重要业务恢复时间目标不得大于 4 小时，重要业务恢复点目标不得大于半小时。如今我国银行业在主备方式的基础上，正逐步向双活、多活的模式发展，以同城和异地灾备的方式来保护其宝贵的资产——数据。

11.2.1 我国银行业务连续性管理的现状

近年来，我国银行业业务发展迅猛，大型银行的资本总额、开户数量、业务处理量已位居世界前列，经营范围遍及全国并在国外快速扩张，一旦业务停顿，可能影响全行乃至整个金融体系的正常运转，并影响社会稳定。因此，在数据大集中后，国家、银行业监管机构及银行企业自身对灾难恢复、业务连续管理的重视程度越来越高。一方面，政府、央行及银监会对于银行机构的应急管理和业务连续运作提出了更为明确、更为细致的要求；另一方面，银行自身也在积极推进灾难恢复、应急管理和信息技术服务持续性管理有关工作，逐步完善业务连续性预案。

1）初步构建了信息系统应急管理体系。确立了应急管理组织架构，区分信息系统突发事件等级，形成统一的应急响应流程和通知报告程序。并注重与地方政府、新闻媒体的沟通协调，加强机构内部各职能部门的协调配合，及时向公众披露信息，增强了突发事件的应对处置能力。

2）积极开展灾难备份系统建设工作。按照“统筹规划、资源共享、平战结合”的原则，大型和股份制银行积极推进“两地三中心”的建设，建立了同城和异地灾备中心，应对建筑类故障和区域性（如地震、洪灾、战争等）灾难。大多数商业银行基本建立了核心业务的灾难恢复系统，保障核心业务数据安全和灾难发生时核心业务的恢复。

3）提升危机处理能力。积极开展应急演练和灾难恢复演练，加强银行内部各部门，以及银行与通讯、电力等外部机构的联防协作。实施了包括核心系统在内的重要业务系统切换演练，提高银行应对信息系统突发事件的能力和信心。

但整体来看，我国银行业在业务连续性管理方面依然存在一些不足。

一是对业务连续性管理的重要性和价值认识不足，尚未形成有效的业务持续管理管理体系。部分银行对业务持续性管理缺乏必要的理解，认为“投入大、收益小”，对金融服务的持续性与公众生活、经济社会正常运转的紧密关系缺乏足够的认识，银行改善业务持续管理的动力大多来自国家或监管政策压力，主观意愿不足，将业务持续性管理等同于信息系统的灾难恢复、日常故障处置的模糊意识大量存在，参与的多为信息技术部门、部分人员，业务连续性计划仅作为事件处理的应急预案，未建立起业务持续管理的管理组织体系，业务持续管理依然游离在企业的日常经营管理活动之外。

二是应急预案体系不够完整，业务应急机制匮乏，外部应急协调不足。大多数银行没有业务层面应急管理机制的开发和演练，场地应急、人员应急等业务持续管理的重要环节缺乏实质性的建设。信息系统应急预案流于形式，不少银行对业务连续性的认识不足，认为业务连续性就是信息系统应急恢复，就是科技部门的责任，没有在全行层面建立整体管理体系，缺乏科技与业务、公关等部门的联动，缺少业务应急手段和客户安抚、媒体公关等处理措施。业务部门配合不足、业务人员参与力度不大、业务覆盖面不全，一旦出现意外，应急预案可能无法发挥作用，与外部机构（如政府机构、公共事

业机构、银行同业、外部合作金融服务机构等）的协作联动不足。多数银行业务连续性演练仅停留在信息科技层面，缺乏涵盖业务、技术和后勤保障等多方面的全行性演练，导致应急和灾备能力有效性无法得到验证。

三是业务的灾难恢复目标不明确、信息系统灾备覆盖面不够、灾备资源的有效性保障不足，存在缺乏风险评估和业务影响分析，缺乏对业务中断损失与灾备建设投入的成本效益测算，导致灾备系统、科技应急体系建设盲目投入、缺乏规划，灾备系统覆盖不足等问题。虽然银行大多已建立了灾备中心，但是业务分类分级及差异化的业务恢复目标还不十分明确，部分银行灾备中心只停留在核心账务数据保护的层面，一旦发生灾难，很难实现重要交易渠道的恢复、重要客户及交易数据的恢复。灾备切换演练未能真正贴近实战，灾备人员配置、系统演练有效性验证等方面存在不足。

11.2.2 加强银行业务连续性管理的意义

信息科技连续运作的根本目标是保障业务的持续性，商业银行更应从业务角度出发，以业务持续为目标，形成应对突发事件、灾害灾难的各部门协同管理体系，加强顶层设计。随着经济、金融全球化和信息技术的发展加速，信息科技的广泛应用使得金融机构之间的关联度大大提升，各个国家金融机构间的外部依赖度也不断加强，单家机构的故障可能使关联金融机构遭受损失，并且风险扩散的速度更快、范围更大，外部性大大增强，因此推动和加强银行业的业务连续性体系建设，从全行层面进行规划，进一步加强整体业务连续性规范和深层次机制建设，实现对各种事故和灾难的有效应对，维护正常的经济金融运行秩序非常迫切。

从长远来看，业务持续管理的价值并非仅仅是企业应对灾难、提高生存能力的工具，在许多发达国家金融行业，业务持续管理已成为改善经营管理、承担社会责任的基本准则，是银行提高风险预测和快速应对能力，适应需求变化和威胁，保持竞争优势的重要基础。可以说，业务连续性管理直接关系到中国银行业的国际竞争力，对整个行业长期、可持续的健康发展具有深远的意义。

11.2.3 《商业银行业务连续性监管指引》解读

银监会在充分借鉴新加坡金管局《SINGAPORE STANDARD SS 507》、英国《BSI PAS 56》及一些国际先进银行的业务连续性管理经验基础上，结合我国国情和商业银行实际情况，于2011年12月28日正式发布了《商业银行业务连续性监管指引》（银监发［2011］104号）（下称《指引》）。

1.《指引》的主要内容和要求

《指引》以提高商业银行业务连续性管理能力，降低业务中断产生的影响，快速恢复业务为目标，要求商业银行建立业务连续性管理体系，规范了相关组织架构和工作流程，明确了业务影响分析、风险评估的方法和工作重点，对业务连续性计划的内容、演

练，业务中断事件的应急处置过程提出了具体要求，推动商业银行加强各部门的协同保障，建立业务连续性管理持续改进机制。《指引》更加强调商业银行在应对业务运营中断事件时进行统筹管理，促进各部门的协同，提高应急的能力。同时，还明确了银监会应对商业银行业务运营中断事件的应急处置方法和流程，强化了监管机构与银行间、金融同业间、监管机构与外部其他部门间的应急协同。《指引》包括以下几个方面：

1）总则要求与组织体系。在总则中提出了业务连续性管理的内容、目标、范围及原则，强调以履行社会责任为开展业务连续性管理活动的基本原则，不能仅单纯从银行业务收益角度考虑，并强调以人为本、重要业务优先保障、内外部门间的协同等原则。商业银行应当将业务连续性管理纳入全面风险管理体系，建立业务连续性日常组织架构和应急管理组织架构，商业银行董（理）事会应作为业务连续性管理的决策机构，承担最终责任。《指引》强调商业银行应建立业务持续管理（Business Continuity Management，BCM）的组织框架，设立负责 BCM 的部门并能从整体上协调全行其他部门，该部门应为风险部或办公室等综合管理部门而非信息科技部门。在 BCM 组织框架下，业务和科技部门应作为业务连续性的执行部门，尤其是业务部门应负责设定业务恢复指标、创立业务恢复计划、建立业务恢复资源等，强调了以业务为主体的连续性管理职能及业务部门在全行业务连续性建设中的义务和重要作用。

2）业务影响分析。强调业务连续性管理是对银行业务的识别、分析、量化指标的过程，是制定业务连续性管理的策略及规划的重要手段。业务影响分析应从识别重要业务入手，明确重要业务的归口部门，量化业务中断对银行的影响，分析业务恢复指标，明确业务运作所依赖的关键资源中断的影响范围及恢复指标。商业银行在业务影响分析过程中，应关注业务部门与业务条线之间的对应关系，关注业务之间的依赖关系，关注重要业务与关键资源的对应关系。《指引》明确提出商业银行重要业务恢复时间目标与恢复点的指标要求，重要业务恢复时间要求包括资源恢复时间和处置决策过程、业务验证过程等。

3）业务连续性计划与资源建设。商业银行应建立覆盖所有重要业务和应对大范围业务运营中断的总体应急预案，以及针对不同场景的专项应急预案，应注重总体应急预案与专项应急预案之间的关系，业务预案应关注与其他预案之间的衔接，做到全行应急“一盘棋”，并将外部供应商、金融同业及其他外部机构纳入业务连续性计划范围。在业务连续性计划所需资源建设方面，不仅要加强在应急及恢复过程中的备份资源建设，还应加强信息系统在日常生产中的高可用性建设，减少系统中断的概率。

4）业务连续性演练与持续改进，它是业务连续性计划、预案、资源是否有效的验证和保障。一方面，商业银行要保障演练的计划性与针对性，应把演练作为一项日常工作来有计划的、定期开展，要针对重要业务中断场景、重大业务活动、重大社会活动等关键时点开展演练；另一方面，要保障演练的实操性与全面性，商业银行应注重以真实业务接管为目标，开展全行性演练并将外部供应商、基础设施保障单位等纳入演练范畴，三年内应实现所有重要业务的演练全覆盖。在评估与改进方面，商业银行应做到评估与审计、内外部评估、全面与专项审计相结合，及时发现问题和改进。

5）运营中断事件应急处置。首先，在业务的监测与预警方面，商业银行需建立自动化、智能化的监测手段，从单纯信息系统监测向业务监测发展，从被动监控到主动监控，加强关键业务时点的系统压力监测，建立科技与业务部门间、银行与外部单位间的风险信息提示与共享。其次，在事件处置阶段，不仅要按照一体化应急流程，对事件实施分级分类处置，更应关注业务应急处置措施的运用。要按照业务应急预案，通过减少服务功能、缩小服务范围，保障关键、紧急的业务处理，或利用替代系统、手工记账、分支机构或他行支付渠道等手段进行业务应急处置，加强对外沟通，最大程度降低负面影响，而非一味等待信息系统的恢复。再次，在应急及灾难恢复中，银行应加强危机管理，指派专门的部门负责危机处理，加强舆情监测、信息沟通和发布，以消除或降低负面影响。国外经验表明，发生重大事件后，一些银行不是因为中断造成的损失而难以为继，而是因为丢掉了客户的信任、丧失信誉才逐步走向衰落。

《指引》旨在“强化事前监管要求、建立事中处理流程、明确事后报告路径”，它是银监会在日常监管与银行突发事件处置中的指导与监管工具，也是目前我国在“业务连续性”管理领域的第一份监管指引。

2. 各商业银行加强业务连续性管理的建议

各商业银行在积极推进《商业银行业务连续性监管指引》的贯彻落实过程当中，应积极加快建立和完善银行业金融机构业务连续性管理体系，充分借鉴和引进国际先进实践和标准规范，加强组织建设，明确责任、落实工作职责，科学制订业务连续性计划，系统地推进灾备系统、应急体系建设，积极开展应急演练。建立常态化评估维护机制，形成企业的业务连续性管理文化，使每个员工建立防灾意识，自觉自愿的参与到银行的业务连续性管理各流程活动中。

1）加大力度推进银行业金融机构的应急演练工作，积极开展银行业行业性应急演练和金融跨业应急演练工作。鼓励金融机构进行业务连续性管理的演练活动，组织协调由金融管理部门、基础设施供应商和多个金融机构参与的联合演练活动，持续提高金融机构业务连续性管理的实践能力，增强我国金融业的整体业务持续性能力。

2）加强与行业外其他政府部门的应急协调，建立有效的应急协作联动机制。虽然国家各有关部门建立了应对突发事件的应急预案和组织机构，但部门间的条块分割管理使协调较为困难，难以形成合力，极大地影响了应急效能。在金融全球化、综合化、信息化发展的大趋势下，应充分借鉴国外先进实践。对内，要深入推动银行、证券、保险建立有效的应急联动处置机制，制定金融业联合应急预案，成立跨业的应急处置小组，加强信息沟通、资源共享、统一协调，提高处置能力；对外，要加强银行与电力、电信、公安等部门的信息交流，建立风险监测预警机制，整合信息源，积极开展风险分析和预警；制定金融业与其他政府部门的跨业应急预案，提高行业整体的应对突发事件能力和水平。

3）建立银行业业务持续性管理的评估和持续改进机制。要建立对监管部门、银行业金融机构的业务持续性管理计划和活动的评估维护程序，发现问题并持续改进质量。要研究建立银行业金融机构业务持续性管理的成熟度模型，促使银行业的业务持续运作

能力从初级阶段达到高度协调、可衡量，具备高度成熟、能应对百年一遇甚至更高标准突发事件的能力。

11.3 灾难恢复管理的组织结构

《银行业信息系统灾难恢复管理规范》中要求组织机构设立职责，提出灾难恢复组织机构应分为决策层、管理层和执行层，在灾难恢复工作中，分别承担重大事宜的决策、恢复工作的管理和协调、恢复工作的具体实施等不同职责。

银行应结合其日常组织机构的具体情况建立灾难恢复规划组织机构，并明确其职责。其中一些人可负责两种或多种职责，一些职位可由多人担任（灾难恢复预案中明确他们的继任顺序）。

灾难恢复规划的组织机构由管理、业务、技术和行政后勤等人员组成，分为灾难恢复规划领导小组、灾难恢复规划实施组和灾难恢复规划日常运行组。其中，实施组的人员在实施任务完成后可成为日常运行组的成员。银行也可聘请外部专家协助灾难恢复规划工作，还可委托外部机构承担实施组和运行组的部分或全部工作。

灾难恢复管理组织结构的职责如下。

1. 灾难恢复规划领导小组

灾难恢复规划领导小组是实施灾难恢复规划工作的组织领导机构，组长应由单位高层领导担任，领导和决策灾难恢复规划重大事宜，其主要职责如下：

1）审核并批准经费预算。

2）审核并批准灾难恢复策略。

3）审核并批准灾难恢复预案。

4）组织灾难恢复预案的测试和演练。

5）批准灾难恢复预案的执行。

2. 灾难恢复规划实施组

灾难恢复实施组的主要职责是负责：

1）灾难恢复的需求分析。

2）提出灾难恢复策略和等级。

3）灾难恢复策略的实现。

4）制定灾难恢复预案。

3. 灾难恢复规划日常运行组

灾难恢复日常运行组的主要职责是负责：

1）灾难备份中心日常管理。

2）灾难备份系统的运行和维护。

3）灾难恢复的技术支持。

4）灾难恢复预案的教育、培训和演练。
5）维护和管理灾难恢复预案。
6）突发事件发生时的损失控制和损害评估。
7）灾难发生后信息系统和业务功能的恢复。
8）灾难发生后的外部协作。

11.4 灾难恢复管理流程

业务连续性/灾难恢复管理体系建设是一项复杂的系统工程，需要充分借鉴国内外先进经验，遵循成熟的标准规范，根据自身组织机构特点和信息系统建设实际情况灵活建设。关于信息系统灾难备份与恢复，西方发达国家积累了丰富的经验，建立了比较成熟的标准体系，如国际灾难恢复协会（DRII）的《业务连续性规划师专业实践》、信息系统审计与控制协会（ISACA）的《COBIT 管理指南》等；我国也制定了相关的标准规范，如《信息安全技术信息系统灾难恢复规范》（GB/T 20988—2007）、《信息安全技术信息安全风险评估规范》（GB/T 20984—2007）等。

为了规范和引导银行业信息系统灾难恢复工作，有效防范银行业信息系统风险，保护银行业客户的合法权益，中国人民银行在继承国际先进标准和国家标准的基础上，针对银行业信息系统、业务流程、组织体系、监管要求的特点，制定并发布了金融行业标准《银行业信息系统灾难恢复管理规范》（JR/T 0044—2008），该标准成为我国银行业信息系统灾备体系建设的重要指导性文件。

银行信息系统的灾难恢复工作，不仅包括灾难恢复规划和灾难备份中心的日常运行，还包括灾难发生后的应急响应、关键业务功能在灾难备份中心的恢复和重续运行，以及生产系统的灾后重建和回退工作。其中，灾难恢复规划是一个周而复始、持续改进的过程，包含以下几个阶段。

（1）灾难恢复需求的确定 灾难恢复需求分析步骤包括风险分析（RA）、业务影响分析（BIA）和确定灾难恢复目标 3 个子步骤，通过需求分析这 3 个子步骤了解信息系统的风险，对业务进行综合考虑并确定关键业务功能及恢复的优先顺序和灾难恢复 RTO/RPO 灾难恢复时间范围指标。

（2）灾难恢复策略的制定 灾难恢复策略制定步骤根据风险和损失平衡的原则，确定每项关键业务功能的灾难恢复策略，并将这些策略正式文档化。

（3）灾难恢复策略的实现 灾难恢复策略实现步骤根据灾难恢复的策略，选择和建设灾难备份中心、实现灾备系统技术方案并实现其技术支持和维护能力。

（4）灾难恢复预案的制定、落实和管理 灾难恢复预案的制订和管理步骤负责编制灾难恢复预案，对灾难恢复预案进行教育、培训和演练，并负责灾难恢复预案的保存、分发及维护和变更管理。

这些步骤代表了一个全面的灾难恢复管理能力的关键要素。整个开发过程的责任是

由灾难恢复实施组所具体负责。

11.4.1 灾难恢复需求分析

灾难恢复需求分析需要从风险分析（RA）、业务影响分析（BIA）和确定灾难恢复需求 3 个方面来进行分析。

1. 风险分析

风险分析是指标识信息系统的资产减值，识别信息系统面临的自然的和人为的威胁，识别信息系统的漏洞，分析各种威胁发生的可能性，并定量或定性描述可能造成的损失。通过技术或管理手段，防范或控制信息系统的风险。依据防范或控制风险的可行性和残余风险的可接受程度，确定对风险的防范和控制措施。

（1）确定风险分析目标 银行应根据长期可持续发展和信息化建设的战略目标，明确风险分析目标，全面识别信息系统灾难风险的威胁和脆弱性。

（2）确定风险分析范围

1）根据信息系统的范围和特点，全面识别和分析影响信息系统正常运行的灾难风险要素。

2）根据信息系统支持业务的区域范围，分析信息系统面临的区域性灾难风险。

3）根据业务经营领域，分析信息系统中断造成的金融领域关联性风险。

（3）风险分析的方法

1）资产识别：主要包括基础设施、硬件、软件、数据、文档、服务和声誉等，银行应根据资产对业务正常运作的不同影响程度，确定资产的等级。

2）威胁识别：指对信息资产构成潜在破坏的可能性因素，包括自然或人为、有意或无意、可控或不可控等。

3）脆弱性识别：脆弱性是可能被威胁利用的信息资产弱点。脆弱性识别可以从环境、业务、网络、系统、应用等层次进行识别。脆弱性识别的依据可以是国际或国家的安全标准，也可以是行业规范、应用流程的安全要求。

4）风险计算：风险计算是采用适当的方法与工具确定威胁利用脆弱性导致信息系统灾难发生的可能性，如根据威胁出现的频率及脆弱性状况，计算威胁利用脆弱性导致灾难发生的可能性；根据资产重要程度及脆弱性严重程度，计算灾难发生后的损失；根据计算出的灾难发生的可能性及灾难的损失，计算风险值，并进行风险等级划分等。

（4）风险控制 评估现有安全策略和措施的有效性，确定信息系统仍然可能存在的风险，即残余风险。

银行应根据资产等级及残余风险发生的概率、可能造成的损失和风险防范成本，评估风险可接受的程度，确定可接受的风险。针对不可接受的风险，确定风险防范措施，并定期评估残余风险。

2. 业务影响分析

通过风险分析，得到存在风险的组织机构业务系统范围，而业务影响性分析则进一

步结合业务和灾难恢复具体要求，分析业务功能和相关资源配置并评估中断影响，为进一步制定灾难恢复策略提供基础和依据。

（1）业务功能分析 通过业务功能分析，确定业务功能的关键程度，主要包括：

1）政策性：业务功能的政策要求。

2）业务性质：核心业务或非核心业务。

3）业务服务范围：涉及的内外部机构、用户等范围。

4）数据集中程度：业务数据的集中与处理的集中、地域分布。

5）业务时间敏感性：实时与非实时业务、业务运行时段和用户使用频度。

6）业务功能的关联性：与其他业务功能及其他机构业务功能之间的关联程度。

（2）评估业务中断影响

1）分析业务功能和相关资源配置：分析单位的各项业务功能及各项业务之间的相关性，确定支持各种业务功能的相应信息系统资源及其他资源，明确相关信息的保密性、完整性和可用性要求。

2）评估中断影响：应采用定量和/或定性的方法，对各种业务功能的中断造成的影响进行评估。定量分析是以量化方法，评估业务功能的中断可能给单位带来的直接经济损失和间接经济损失；定性分析是以非量化方法，评估业务功能的中端可能对国家的政治、社会、法律及单位内部事务等造成的影响。

业务影响分析是灾难恢复管理的一个关键步骤，使灾难恢复规划实施组能对系统要求、过程和相互依赖性进行完全的特征化，并且使用这些信息确定连续性要求和优先级。业务影响分析的目的是将特定的系统组建同其所提供的关键服务相关联，并基于这些信息特征化中断对系统组件的结果。业务影响性分析得出的结论应相应综合至组织机构的灾难备份管理策略中。

3. 确定灾难恢复需求

信息技术系统可以是一个包含各种组件、接口和进程的非常复杂的系统。系统通常有多种使命，因此对系统服务或能力的重要性也会有不同的理解。业务影响分析的第一个步骤是评估信息技术系统，以确定由系统执行的关键功能并标识执行它们所需的特定系统资源。

（1）确定需求等级 首先需要确定灾难恢复的需求等级。

（2）确定最低恢复要求 根据信息系统的时间敏感性，确定信息系统灾难恢复目标的最低要求，例如：

1）第一类：RTO < 6 小时，RPO < 15 分钟

2）第二类：RTO < 24 小时，RPO < 120 分钟

3）第三类：RTO < 7 天

（3）确定恢复优先级 根据业务功能分析、业务中断影响分析并综合考虑系统间的依赖性，确定信息系统的恢复优先级。

（4）确定相关资源 银行应确定灾难恢复所需的 7 个方面资源要素：

1）数据备份系统。

2）备用数据处理系统。
3）备用网络系统。
4）备用基础设施。
5）技术支持能力。
6）运行维护管理能力。
7）灾难恢复预案。

11.4.2 灾难恢复能力等级及策略的制定

1. 灾难恢复能力等级

2008 年，中国人民银行发布了《银行业信息系统灾难恢复管理规范》，其中规定了灾难恢复能力等级及其确定方法，银行应根据信息系统的 RTO 和 RPO 要求，确定信息系统的灾难恢复能力等级，如表 11-1 所示。

表 11-1 RTO/RPO 与灾难恢复能力等级的关系

灾难恢复能力等级	RTO	RPO
1	2 天以上	1 ~ 7 天
2	24 小时以上	1 ~ 7 天
3	12 小时以上	数小时至 1 天
4	数分钟至 2 天	数小时至 1 天
5	数小时至 2 天	0 ~ 30 分钟
6	数分钟	0

2. 灾难恢复策略的制定

灾难恢复策略的制定就是按照灾难恢复资源的成本与风险可能造成的损失之间取得平衡的原则，即“成本风险平衡原则”确定每项关键业务功能的灾难恢复策略，不同的业务功能可采用不同的灾难恢复策略。具体的灾难恢复策略如下。

（1）成本风险分析和策略的确定 银行应按照成本风险平衡原则，确定每项关键业务功能的灾难恢复策略，不同业务功能可采用不同的灾难恢复策略。主要包括灾难恢复建设计划、灾难恢复能力等级、灾难恢复建设模式、灾难备份中心布局。

灾难恢复能力等级包括灾难恢复能力等级的确定、最低的灾难恢复能力等级要求、灾难备份中心的布局、资源服务的获取和保障等。

1）灾难备份中心的布局原则：灾难备份中心应设置在中华人民共和国境内；应保证灾备中心与生产中心之间距离合理；应避免灾备中心与生产中心同时遭受同类风险；应综合考虑灾备中心所在地的技术支持能力、电讯资源、地理地质环境、公共资源与服务配套能力等外部支持条件。

2）布局模式：可以采用一主一备、一主多备、互为备份、多主一备、混合等方式。

（2）资源、服务的获取和保障

1）资源的获取。

2）基础设施：包括机房和其他辅助设施，通常可以采用自建的方式或者共享的方式来获取。

3）数据备份系统、备用数据处理系统：是用于灾难恢复的数据备份系统和备用数据处理的系统设备，可以通过自行采购、与供应商签订紧急供货协议、租赁、外包等方式获得。

4）通信网络：用于灾难恢复的通信网络包括生产中心和备份中心间的备份网络和最终用户访问灾难备份中心的网络，一般采用自行建设和租用运营商线路的方式获取。

5）专业服务的获取。

6）灾难恢复咨询服务：包括风险分析、业务影响分析、灾难恢复策略制定、灾难备份中心规划与建设、灾难恢复预案制定、测试、培训和演练等，通常采用委托外部咨询机构和联合外部咨询机构的方式获取。

7）灾难恢复技术支持服务：服务对象包括数据备份系统、备用数据处理系统和通信网络等，其获取方式包括自有技术支持队伍、专业服务提供商、设备提供商等。

8）灾难恢复运营管理服务：包括灾难备份中心的日常运行维护和灾难恢复预案的维护等，其获取方式包括自主运行维护、外包。

9）外包的管理：灾难恢复服务外包时应符合国家和行业的相关服务资质要求，并至少满足以下要求：

① 应熟悉银行业信息系统架构和业务流程，具有灾难恢复外包服务的成功案例和实践经验。

② 应具有完备的信息安全管理体系和服务质量保证体系，并通过 ISO/IEC 27001、ISO/IEC 9001 等认证。

③ 应独立运营管理灾难备份中心，且机房的可用性应至少达到 99.9%，其所能提供的灾难恢复能力等级应达到 5 级（含）以上。

11.4.3 灾难恢复策略的实现

灾难恢复策略的实现步骤就是根据灾难恢复的策略，选择和建设灾难备份中心，实现灾备系统技术方案、技术支持和维护能力。灾难恢复策略实现的具体要求如下。

1. 灾难备份中心的选择和建设

1）选址原则：选择或建设灾难备份中心时，应根据风险评估的结果，避免灾难备份中心与生产中心同时遭受同类风险。灾难备份中心还应具有方便灾难恢复人员或设备到达的交通条件，以及数据备份和灾难恢复所需的通信、电力等资源。

2）基础设施的要求：在新建或选用灾难备份中心的基础设施时，计算机机房应符合 GB/T 2887—2000 的要求；工作辅助设施和生活设施应符合灾难恢复目标的要求。

2. 灾难备份系统技术方案的实现

1）技术方案的设计：根据灾难恢复策略制定相应的灾难备份系统技术方案，包含

数据备份系统、备用数据处理系统和备用的网络系统。技术方案中所涉及的系统，应获得同生产系统相当的安全保护并具有可扩展性。

2）技术方案的验证、确认和系统开发：为确保技术方案满足灾难恢复策略的要求，应由单位的相关部门组织对技术方案进行确认和验证，并记录和保存验证及确认的结果。按照确认的灾难备份系统技术方案进行开发，实现所要求的数据备份系统、备用数据处理系统和备用网络系统。

3）系统安装和测试：按照经过确认的技术方案，实施组应制订各阶段的系统安装和测试计划，以及支持不同关键业务功能的系统安装和测试计划，并组织最终用户共同进行测试。确认以下各项功能可正确实现：数据备份及数据恢复功能；在限定的时间内，利用备份数据正确恢复系统、应用软件及各类数据，并可正确恢复各项关键业务的功能；客户端可与备用数据处理系统正常通信的功能。

4）技术支持能力的实现：单位应根据灾难恢复策略的要求，获取对灾难备份系统的技术支持能力。灾难备份中心应建立相应的技术支持组织，定期对技术支持人员进行技能的教育和培训。

5）运行维护管理能力的实现：为了大到灾难恢复目标，灾难备份中心应建立各种操作和管理制度，用以保证数据备份的及时性和有效性；保证备用数据处理系统和备用网络系统处于正常状态，并与生产系统的参数保持一致；保证有效的应急响应、处理能力。

6）灾难恢复预案的实现：灾难恢复的每个等级均应按我国灾难恢复等级划分的具体要求，制定相应的灾难恢复预案，并进行落实和管理。

11.4.4 灾难恢复预案的制定和管理

银行在设计灾难恢复预案时，首先需要设计灾难恢复预案框架，即至少要包含《银行业信息系统灾难恢复管理规范》中所描述的组织、流程和资源等预案主要内容，然后需要设计灾难恢复预案的文档形式。预案应由两部分组成：第一部分是灾备体系建设，主要介绍发生灾难之前的灾备体系建设工作，包括策略制定、组织机构落实和资源配置等；第二部分是灾难恢复流程，主要介绍发生灾难后，为了恢复信息系统的重续运行，灾备中心进行响应及恢复的工作流程。

具体灾难恢复预案应按照《银行业信息系统灾难恢复管理规范》对演练目的、形式、层次、组织实施、评估和预案修订来进行指导，灾难恢复预案制定和管理步骤负责编制灾难恢复预案，对灾难恢复预案进行教育、培训和演练，并负责灾难恢预案的保存、分发及维护和变更管理。

1. 灾难恢复预案的制定

银行应结合自身实际情况编写灾难恢复预案，灾难恢复预案应包括应急预案和信息系统灾难恢复预案。

（1）应急预案 至少应包括：

1）灾难场景定义、目标和范围。

2）应急管理组织机构。

3）应急恢复决策及授权，包括应急恢复条件、权限、处置策略及强制决策点等。

4）应急相应工作规程，包括紧急事件初始响应、损害评估、指挥中心成立和人员召集、灾难预警、灾难宣告、启动灾难切换流程等。

5）应急管理工作中使用的各项文档，包括通讯录、工作文档、应急工具等。

（2）信息系统灾难恢复 至少应包括：

1）灾难恢复范围和目标。

2）灾难切换规程。

3）灾后重续运行操作指引。

4）各系统灾难切换操作手册。

（3）灾难恢复预案的制定 应遵守以下原则：

1）完整性：灾难恢复预案应包含灾难恢复的整个过程，以解灾难恢复所需的尽可能全面的数据和资料。

2）易用性：预案营运易于理解语言和图表，并适合在紧急情况下使用。

3）明确性：预案应采用清晰的结构，对资源进行清除的描述，工作内容和步骤应具体，每项工作应责任明确。

4）有效性：预案应尽可能满足灾难发生时进行恢复的实际需要，并保持与实际系统和人员组织的同步更新。

5）兼容性：灾难恢复预案应与其他应急预案体系有机结合。

（4）灾难恢复预案制定的过程

1）初稿的制定：按照风险分析和业务影响分析所确定的灾难恢复内容，根据灾难恢复登记的要求，结合单位其他相关的应急预案，撰写出灾难恢复预案的初稿。

2）初稿的评审：单位应对灾难恢复预案初稿的全面性、易用性、明确性、有效性和兼容性进行严格的评审。评审应有相关的流程保证。

3）初稿的修订：根据评审结果，对预案进行修订，纠正在初稿评审过程中发现的问题和缺陷，形成预案的修订稿。

4）预案的测试：应预先制订测试计划，在计划中说明测试的案例。测试应包含基本单元测试、关联测试和整体测试。测试的整个过程应有详细的记录，并形成测试报告。

5）预案的审核和批准：根据测试的记录和报告，对预案的修订稿进一步完善，形成预案的报批稿，并由灾难恢复领导小组审核和批准，确定为预案的执行稿。

2. 灾难恢复预案的演练

演练是为了验证灾难恢复预案的完整性、易用性、明确性、有效性和兼容性，提高银行灾难恢复预案的执行力。

（1）演练的形式 演练有事前通告和非事前通告两种方式，主要包括：

1）桌面演练：组织相关的灾难恢复组织机构人员，以会议形式模拟各种灾难场

景。这种演练方式主要是验证灾难恢复预案的决策和指挥能力。

2）模拟演练：模拟灾难场景，利用灾难备份系统和灾难恢复预案模拟系统切换和业务恢复，通常不涉及真实的业务操作。

3）实战演练：模拟灾难场景，利用灾难备份系统和灾难恢复预案完成系统切换和业务恢复，涉及真实的业务操作，银行在演练完成后需进行数据和环境的回导。

（2）演练的层次主要包括：

1）以指挥协调为主的指挥演练。

2）以技术操作为主的技术演练。

3）以业务恢复为主的业务演练。

（3）演练的组织实施

1）应预先对培训需求进行评估，开发和落实相应的培训/教育课程，保证课程内容与预案的要求相一致。

2）应事先确定培训的频次和范围，事后保留培训的记录。

3）预先制订演练计划，在计划中说明演练的场景。演练的整个过程应有详细的记录，并形成报告。

4）灾难恢复演习应保证至少每年一次。

（4）演练的评估 演练完成后应针对演练的组织、过程和效果进行评估，主要包括：

1）灾难恢复预案的有效性和可用性。

2）演练结果与演练目标的差距。

3）演练过程中发现的生产系统和灾难备份系统存在的问题。

4）演练工作的组织能力。

5）参演人员的应急能力。

6）应急资源的协调保障能力。

（5）演练后预案的修订 应根据演练评估结论对灾难恢复预案进行维护和更新，并在下次演练中加强对更新部分的演练，验证更新部分的有效性。

3. 灾难恢复预案管理

为了保证灾难恢复预案的有效性，应从以下方面对灾难恢复预案进行严格的变更管理。

（1）保管、更新和分发 经过审核和批准的灾难恢复预案，应具备以下条件：

1）由银行专人负责保存与分发。

2）具有多份拷贝，在不同的地点保存。

3）分发给参与灾难恢复工作的所有人员。

4）在每次修订后所有拷贝统一更新，并保留一套，以备查阅，原分发的旧版本应予以销毁。

（2）更新维护 灾难恢复预案的更新维护，主要包括：

1）业务流程的变化、信息系统的变更、人员的变更都应在灾难恢复预案中得到及

时反映。

2）预案在测试、演练和灾难发生后、实际执行时，其过程均应有详细的记录，并应对测试、演练和执行的效果进行评估，同时对预案进行相应的修订。

3）灾难恢复预案还应定期评审和修订，至少每年一次。

（3）教育和培训 应定期组织灾难恢复预案的教育和培训，采用培训与自我学习方式，通过网络、集中培训、资料传阅等方式，广泛宣传应急措施和预防、避险等常识，增强风险防范意识和应急能力。各有关方面要有计划地对应急实施人员和管理人员进行培训，确保相关人员熟知应急预案，提高其专业技能。培训后应保留培训的记录。

11.5 案例介绍：业务连续性与灾难恢复管理实践

某大型商业银行（以下简称 F 行）非常重视灾难恢复管理体系建设，将其作为全行信息化建设的重点工程。在灾备体系建设过程中充分遵循《银行业信息系统灾难恢复管理规范》的相关规定，结合该行实际情况，规划、设计了完善的灾备体系框架，分设多个灾备项目，合理安排工作任务和工作次序，稳步推进灾备体系建设并取得了丰富成果，有效地提高了风险管控能力，提高了股东、客户和合作伙伴的信心。

1. 成立备援测试中心，明确灾备管理工作定位

灾备体系庞大而复杂，需要多个部门协同工作，是一项长期工程，因此，灾备体系建设工作宜由某个全职部门牵头开展。为有效推进灾备体系建设工作，F 行于 2008 年成立了备援测试中心，下设灾备管理部，全面负责全行灾备体系建设规划和管理。F 行经过分析和研究，明确了灾备管理、应急管理、生产日常管理、信息技术连续性管理和业务连续性管理等概念之间的关系。其中特别需要指出的是，灾备管理应对的是物理性灾难，对于逻辑性灾难，灾备管理无能为力，逻辑性灾难是应急管理的工作范畴。

2. 规划灾备体系建设，明确工作思路

F 行根据全行信息系统架构及部署情况，全方位地规划了灾备体系建设工程，计划按照“3 个层次、5 个项目”的工作思路，全面建设灾备体系。“3 个层次”即总行、一级分行、二级分行等 3 层信息系统部署架构。“5 个项目”即总行数据中心异地灾备项目一期和二期、总行数据中心同城灾备项目、一级分行灾备项目和二级分行灾备项目，其中总行数据中心异地灾备项目一期和二期分别基于现有资源和正在建设当中的某数据中心的资源。F 行计划通过这些项目完成灾备体系初步建设，然后进入持续维护管理阶段，不断演练，不断完善灾备体系。

3. 设计灾备体系框架，建设灾备体系

《银行业信息系统灾难恢复管理规范》将灾难恢复预案定义为信息系统灾难恢复所需组织、流程、资源等预先制定的行动方案，用于指导相关人员在预定的灾难恢复目标内恢复信息系统支持的关键业务功能。F 行根据该定义，综合考虑灾难恢复策略、组织

机构、灾难恢复预案和管理制度等，设计了完善的灾备体系框架。

（1）开展业务影响分析，制定灾难恢复策略 该行按照《银行业信息系统灾难恢复管理规范》要求，根据业务功能分析、业务中断影响分析并综合考虑系统间的依赖性，确定信息系统的恢复优先级，对全行部署的所有信息系统进行了梳理，分析各个信息系统的部署地点、相互之间的依赖关系、所支撑的业务和业务中断的影响程度等，划分各个信息系统的恢复需求等级，排列恢复优先级，并结合当前资源情况，明确了灾难恢复的信息系统范围和恢复时间指标。

F 行在总行层面，采取了“两地三中心”的布局模式，其中异地灾备中心与软件开发和测试复用机房、网络、系统和运行保障等基础资源，充分贯彻《银行业信息系统灾难恢复管理规范》所倡导的成本风险平衡原则。在一级分行和二级分行层面，F 行均采用了“多主一备”的布局模式。

（2）建立灾难恢复指挥体系，明确工作职责 F 行根据《银行业信息系统灾难恢复管理规范》对灾难恢复组织机构的要求，结合本行组织架构，成立了“包含决策层、管理层、执行层”的灾难恢复指挥体系。决策层由高层管理者组成，主要负责批准灾难恢复预案的启动和重大事项决策；管理层由业务、技术、后勤等相关部门负责人组成，在决策层的领导下开展工作，主要负责协调资源并指挥灾难恢复工作；执行层由业务、技术、后勤等相关部门的工作人员和外部机构人员组成，在管理层的领导下开展工作，负责灾难恢复的具体实施及恢复后的运行维护工作。三层组织通过指挥/报告机制、协调机制、联络机制、保障机制等灾难恢复工作机制，确保各层之间、同层各部门之间能够信息传达及时、沟通顺畅，确保灾难恢复工作能够顺利进行。

（3）编制灾难恢复预案，组织灾难恢复演练 F 行根据《银行业信息系统灾难恢复管理规范》的要求设计了灾难恢复预案框架，设计了灾难恢复预案的文档形式，编制了《数据中心信息系统灾难恢复预案》。预案由 3 部分组成：第一部分是灾备体系建设，主要介绍发生灾难之前的灾备体系建设工作，包括策略制定、组织机构落实和资源配置等；第二部分是灾难恢复流程，主要介绍发生灾难后，为了恢复信息系统的重续运行，灾备中心进行响应及恢复的工作流程；第三部分是附录，这里收录了涉及保密信息（如系统、网络的技术配置和操作手册等）、变更频繁（如任务一览表、联络清单等），以及作为工作文档模板（如报告单、命令单等）的内容。这种预案结构的最大优点是第一部分和第二部分内容相对稳定，作为预案主文档可以不必频繁修订，便于预案的维护管理，各分支机构可以参考这个预案框架，结合自身实际情况，重点编制附件部分，然后落地实施。

F 行在搭建灾备系统的同时，编制了相应灾难恢复预案，之后组织了灾难恢复演练。F 行按照《银行业信息系统灾难恢复管理规范》对演练目的、形式、层次、组织实施、评估和预案修订的指导，制订了详细的演练计划，设计了详尽的演练方案模板。模板内容包括演练组织管理和技术配置等演练前准备工作，桌面演练、模拟演练、实战演练的目标与定位，演练流程脚本，预期执行结果，演练风险控制和演练评估标准等具体实施方案，以及演练执行过程中的控制、记录、问题汇总和演练后的总结等。

（4）制定灾备管理制度，维护管理灾备体系 灾备管理制度建设作为灾备体系建设可持续发展和有效运作的重要保障。F 行拟从总行和分行两个层面分别制定《数据中心灾备管理实施细则》和《分行灾备管理实施细则》，并与更高层面的《重大突发事件应急预案》和《信息系统应急管理工作实施细则》等有机衔接。灾备管理制度的主要内容将包括预案管理（如问题管理、变更管理、版本管理及发布管理等）、测试管理、演练管理、灾备项目管理、培训管理、监督管理、灾备系统运维管理、灾难响应与处置管理等。

第 12 章
信息安全审计

随着信息技术在我国银行业中的地位越来越高，信息安全已经成为关系到银行业务能否顺利开展的重要因素。保障信息安全，是一个 PDCA 循环过程。通过信息安全审计的实施可以有效地监控银行信息安全管理的运行情况，以及安全管控措施是否得到有效执行；通过信息安全审计还可以帮助信息安全管理部门优化信息安全管理过程达到持续改进信息安全管理的效果。因此，银行信息安全的审计工作就显得格外重要。本篇主要讲述了银行业信息安全审计简介、组织架构、审计内容、审计流程等方面。

12.1.1 信息安全审计简介

目前，在我国的国家审计机关已经开展的信息系统审计工作中，信息安全审计是其重要内容之一。另外银监会、审计署、人民银行等多个行业监管部门及政策指导部门均已出台相关政策，要求建立信息安全审计制度，规范信息安全审计的开展方式方法。

银行信息系统安全审计的依据一般是采用国际公认的信息安全标准与我国法律、法规、标准相结合的办法，主要包括银监会《商业银行信息科技风险管理指引》、ISO/IEC 27001（GB/T 22080）信息安全管理体系要求、GB/T 22239 信息安全等级保护基本要求及银行自身的信息安全规章制度。

12.1.2 信息安全审计组织

从信息安全策略中“职责分离”的基本要求出发，银行信息安全审计与信息安全控制实施岗位分离是信息安全审计组织设置的基本原则。

（1）信息安全审计领导小组 负责确定银行信息安全审计各有关部门的工作职责，指导、监督信息安全审计工作。

（2）信息安全审计组 负责制订内审计划，报领导小组进行审批，并负责对审核后纠正预防措施的跟踪检查和验证工作。

（3）信息安全审计工作小组 负责按照程序的要求及内审计划实施审核活动，报告审核结果。

基于信息安全组织中关于银行信息安全相关岗位及职责的描述，银行管理层应指定相关人员担任信息安全管理审计的审计组长。审计组长负责以下工作：

1）制订每年的信息安全管理审计工作计划。

2）建立一个理解信息安全管理相关标准、并能进行审计工作的独立内审团队。该团队可以由信息科技部门中有信息安全管理体系内部审计资格的人员组成，或由具备相应信息安全技能的内部审计部门人员或委托外部机构进行。

3）对信息安全审计过程中的质量控制负责。

4）对信息安全审计发现问题的改进措施进行跟踪。

12.1.3 信息安全审计内容

1. 网络层面

网络层面的安全审计对象包括对网络架构、网络设备安全及网络行为的审计，审计数据来自人工收集和技术手段收集等。网络架构主要是对链路、结构及网络配置方面的审计；网络设备安全审计主要是设备层面的安全配置审计；而网络行为审计内容重点是对网络中发生的安全事件、网络异常行为的审计。网络层面具体审计的内容如下。

（1）网络架构安全

1）审计内容：网络的划分、网络间通讯的流程和控制、网络链路的备份、网络安全的设计、网络服务。

2）具体的审计项目：查看网络物理连接图、查看网络逻辑连接图（IP 分配）、使用网络侦测工具进行 IP（网络服务）扫描、查看网络安全设计和实施方案、测试备份网络链路、测试网络路由情况、测试网络负载情况。

3）审计频率：每季度一次。

4）审计方式：人工审计。

（2）网络设备安全

1）审计内容：防火墙、路由器、交换机、网关/网关代理。

2）具体的审计项目：查看防火墙安全日志文件、路由器、交换机、网关、网关代理日志文件，检查防火墙安全配置，查看路由器路由和其他网络配置，查看交换机 VLAN、端口映射、数据流控制等配置，查看网关/网关代理配置。

3）审计频率：每周一次。

4）审计方式：如果系统中具有集中日志收集系统，可利用该系统完成日志信息的收集；如果没有，可采用人工收集。

（3）网络行为监控和检测

1）审计内容：监控系统的运作情况、入侵检测运行情况。

2）具体审计项：查看监控系统和入侵检测系统的安装配置文件、查看监控系统和

入侵检测系统的日志文件、测试监控系统和入侵检测系统的报警机制能否正常运作、测试关键的监控和入侵检测功能（运行非正常操作、测试系统能否捕获和报警）。

3）审计频率：实时监控。

4）审计方式：利用网络中的网络监控和检测系统完成审计数据的收集，结合技术和人工方式完成审计。

2. 系统层面

系统层面的安全审计对象包括系统安全技术、计算机病毒防治、远程访问安全。在对设备层面审计的重点是对各种系统生成的日志、操作日志进行审计。具体审计内容如下。

（1）系统安全技术

1）审计内容：操作系统安全。

2）具体审计项：查看操作系统安全日志文件、查看管理员操作日志文件、查看文件访问记录、对用户权限分配情况进行抽查、进行系统漏洞扫描。

3）审计频率：对用户权限分配情况进行抽查、进行系统漏洞扫描等工作，每季度进行一次；其他工作需每周进行一次。

4）审计方式：利用集中日志管理系统完成日志信息的收集和处理；如果系统中没有集中日志管理系统，可选择人工收集。

（2）计算机病毒防治

1）审计内容：防病毒系统的安装情况、防病毒系统运行情况、系统病毒数据库更新情况、用户病毒数据库更新情况。

2）具体审计项：抽查计算机用户的 PC 机是否安装了系统统一规定的防病毒程序，并检查程序的内部设定、抽查计算机用户 PC 机上的病毒数据库版本、随机测试防病毒系统功能、查看防病毒系统的运行日志文件、检查防病毒系统的病毒数据库的版本。

3）审计频率：查看防病毒系统的运行日志文件、检查防病毒系统的病毒数据库的版本等工作，需要每周进行一次，其他工作每季度一次。

4）审计方式：人工收集和审计。

（3）远程访问安全

1）审计内容：远程访问身份验证、远程访问权限分配、远程访问通讯加密、远程访问性能、远程访问服务器和系统的安全性。

2）具体审计项：查看远程访问安全日志文件、查看远程访问控制设定、查看远程访问服务器的性能日志文件、对远程访问服务器进行漏洞扫描、对传送的数据实行电子侦听测试。

3）审计频率：对远程访问服务器进行漏洞扫描、对传送的数据实行电子侦听测试等工作，每季度进行一次，其他工作需每周进行一次。

4）审计方式：人工收集和审计。

3. 应用层面

应用层面的安全审计重点是对应用系统生命周期管理的审计，包括应用软件开发安

全、应用系统运行安全、数据库安全、数据备份和恢复等方面。具体审计内容如下。

（1）软件开发安全

1）审计内容：软件开发环境、软件测试规定和执行情况、软件开发文档管理规定和执行情况、测试系统的升级。

2）具体审计项：查看软件开发规范、查看软件开发环境设计和实施方案、抽查软件开发项目文档和有关技术文档、抽查软件测试记录、查看软件开发系统的备份记录、查看测试系统升级（升级到生产系统）计划和有关实施文档。

3）审计频率：系统上线前。

4）审计方式：人工收集及审计。

（2）应用系统运行安全

1）审计内容：业务主机安全性、业务主机备份和恢复。

2）具体审计项：查看业务主机安全日志文件、查看业务主机管理员操作日志文件、查看文件访问记录、查看数据备份记录、进行主机漏洞扫描、检查所有用户的权限分配情况。

3）审计频率：进行主机漏洞扫描、检查所有用户的权限分配情况等工作，需要每季度进行一次，其他工作每周进行一次。

4）审计方式：利用集中日志管理系统完成日志信息的收集和处理；其他的采用人工收集和审计。

（3）数据库安全

1）审计内容：数据库用户设定和权限分配、数据库访问身份验证、数据库完整性、数据库访问性能。

2）具体审计项：查看数据库安全日志文件、查看数据库性能日志文件、查看数据库用户和用户组设定及相应的权限设定、运行数据库健康测试工具，检查数据库内数据和数据关系的完整性。

3）审计频率：查看数据库用户和用户组设定及相应的权限设定、运行数据库健康测试工具，检查数据库内数据和数据关系的完整性等工作，需要每季度进行一次，其他工作需每周进行一次。

4）审计方式：利用集中日志管理系统完成日志信息的收集和处理；其他的采用人工收集和审计。

（4）数据备份和恢复

1）审计内容：数据备份和恢复计划及执行情况、备份应用程序、备份介质管理制度及执行情况、备份和恢复操作制度及执行情况。

2）具体审计项：查看备份应用程序的运行日志文件、查看备份介质记录、查看备份介质管理记录、查看备份和恢复操作记录、热机备份测试、RAID 磁盘备份测试、备用机测试、查看离线备份管理记录、离线备份介质可用性测试、离线备份系统可用性测试、备份系统和生产系统切换测试、备份介质存放地点检查。

3）审计频率：查看离线备份管理记录、离线备份介质可用性测试、离线备份系统

可用性测试、备份系统和生产系统切换测试、备份介质存放地点检查等工作，需每季度进行一次；热机备份测试、RAID 磁盘备份测试、备用机测试等工作，每月进行一次，其他工作需每周进行一次。

4）审计方式：人工审计。

4. 业务层面

业务层面的安全重点是对账号集中审计管理，以及对关键业务操作行为的审计。

（1）账号管理

1）审计内容：账号分配情况、账号创建情况、账号变更情况。

2）具体审计项：账号的创建时间、创建人，从账号的创建时间、创建人信息，账号的变更时间、变更人、变更内容，账号冻结、解冻时间、操作人员，从主账号分配给附属账号的分配时间、分配者，主、附属账号的有限期等。

3）审计频率：每季度一次。

4）审计方式：通过集中账号管理系统收集账号的审计数据，如果没有集中账号管理系统便采用人工审计。

（2）账号授权

1）审计内容：账号授权过程、账号当前使用权限。

2）具体审计项：包括账号的访问权限，查询资源的授权访问者，权限的分配时间、分配者等，账号权限变更时间、变更人员、变更内容，账号当前对应的权限是否与该账号所进行操作的对应权限一致。

3）审计频率：每周一次。

4）审计方式：通过集中账号管理系统收集账号的审计数据，如果没有集中账号管理系统便采用人工审计。

（3）登录行为

1）审计内容：成功登录、失败登录、登录顺序。

2）具体审计项：包括什么人用什么账号在什么时间登录了什么系统，什么时间登出等；账号失败登录使用的账号、频率、时间等；同一个账号在一段周期（可设置）内登录业务系统的顺序。

3）审计频率：每周一次。

4）审计方式：通过集中账号管理系统收集账号的审计数据，如果没有集中账号管理系统便采用人工审计。

（4）业务操作

1）审计内容：网络管理行为、数据库操作、关键操作。

2）具体审计项：对在维护工作中使用 FTP/Telnet 的各种操作进行审计，获得全部操作记录和结果，实现 Ftp/Telnet 命令级细粒度访问策略审计；对 Ftp/Telnet 的操作执行回放，还原操作内容，记录与登录者身份不符合的 SQL 命令、应用操作命令或流程，基于对指定的数据库对象（如数据库、表、视图、存储过程等）和指定操作（如创建、修改、添加、删除等）进行审计；基于自定义的关键字进行访问控制和审计，通过审

计输出界面，对 SQL 命令的截获、分析和还原，审计关键操作的结果，实现对主流数据库的审计；对于系统配置数据的删除操作进行审计；通过制定数据库关键字段、关键操作进行审计；根据操作时序顺序对操作行为进行审计；对于关键操作关联操作账号的权限范围进行审计。

3）审计频率：每周一次。

4）审计方式：必须通过业务行为审计手段收集网络管理行为数据，结合人工操作进行审计。

（5）互联网访问行为（此项审计限于严格控制与互联网访问的系统中）

1）审计内容：互联网访问行为。

2）具体审计项：互联网网站访问行为审计，网站发帖（BBS）审计，邮件收发、Webmail 发送审计，FTP、TELNET 维护行为审计，网络游戏、即时通讯、P2P 下载等行为审计。

3）审计频率：每周一次。

4）审计方式：必须通过业务行为审计手段收集网络管理行为数据，结合人工操作进行审计。

12.1.4 信息安全审计流程

信息安全审计的工作应定期化的开展，以及时识别信息安全管理过程中存在的问题及达到持续改进的效果。

1. 制订年度信息安全审计计划

成立信息安全审计组，信息安全审计组组长应编制《信息安全年度审计计划》，确定当年信息安全审计的范围、工作时间、团队的组成，以及年度信息安全审计的开展方式，如内部审计的方式或外包审计的方式，并上报管理层批准。

信息安全审计团队的组建是其中的关键步骤，信息安全审计团队的成员必须保持其审计独立性，信息安全审计人员不得审计与其本人负责的工作相关的内容。

信息安全审计组组长主持内部信息安全管理体系并审核策划活动，信息安全审计组根据策划的结果制订《信息安全内审计划》。

《信息安全内审计划》需规定本年度对各业务、流程或部门的审查频次、预计时间和审查范围。内审频次应取决于其现状和目前管理工作的需要性，并考虑以往审核的结果。必要时，信息安全审计组召开准备会议，组长应召集成员及相关接口人做好审查组织安排及过程策划，信息安全审计组成员要进行交叉审核，即本部门的员工不允许审核本部门。

内审计划在审核实施一周前发放给相关职能部门，计划应包括：

1）审核目的、范围和方式。

2）审核依据、审核日期。

3）内审组成员分工及审核日程安排。

4）要求受审核部门或人员配合的事项。受审部门只允许由与该部门业务无直接关系的内审人员审核。

在发生下列情况时，通过管理层批准可进行追加审计：

◇ 发生重大信息安全事故时。

◇ 其他管理层认为需要追加审计的原因。

2. 执行信息安全审计的任务

执行信息安全审计任务的主要工作包括相关会议的召开、现场工作及信息安全审计发现的确认。信息安全审计团队通过访谈、审阅相关资料、现场检查、测试等相关审计方法，检查银行当前信息安全管理的运行情况。在信息安全审计任务执行完以后，需针对审计发现启动纠正预防措施流程，对在审计中发现的问题进行整改。

信息安全审计组组长必要时应在现场审核前召开首次会议阐明内审目的、范围和依据；明确各部门的审核陪同人员，征求受审核部门对内审工作的意见，并对受审查部门提出的异议予以协调。

受审查方须按内审计划委派审核陪同人员，陪同人员应对自身业务有足够了解并能提供见证性文件记录，以配合审核工作的顺利进行。

（1）现场审查

1）取证应按照计划要求进行，无特殊情况，不得随意偏离计划的安排。

2）对于暗示着不符合的线索，即使不在检查之列，也应予以检查，并提出采取改进措施的建议。

3）内审员应正确、合理控制审核结果，客观、公正评价体系的符合性和有效性。

4）现场发现的不符合现象，若不能与受审部门达成一致意见时，应加以记录并确认问题现状后，在末次会议上由内审组长与受审核方沟通后裁决。

（2）审查记录要求

1）关键事件的描述应直接引用其原始信息，不得用主观的综合评述语言。

2）关键事件的记录应保持可追溯性，即记录中应尽量包括其起止时间、地点、人物和文件记录名称、编码、序号，关键事项等。

3）因记录不便或其他不适合情况，可以提取其复印件。

在末次会议上，信息安全审计组应向管理者代表和受审核部门报告审查情况，并由管理者代表（或指定的信息安全审计组长）协调、落实确定的不合格项的纠正或采取改进措施的责任部门。

3. 审计报告

信息安全审计组以“不符合项报告”的形式将不符合项通知到相关责任部门。责任部门收到“不符合项报告”后需尽快分析问题原因，给出纠正和预防措施，并在规定的期限内反馈改进承诺。

在完整的体系内部审核结束后，安全管理小组应总结审核过程及审核发现编制审核报告，报告应包括：

1）审核报告编号、审核的目的、范围和依据。

2）审核日期和方法。

3）内审组成员名单（姓名、部门、职务）。

4）审核结果（不符合项数目、分类及评价）。

5）审核结论（符合性、有效性、适合性及信息安全保证能力）。

6）组长签名及领导批准。

7）附件目录（审核日程计划、不符合项报告、签到表等）。

8）分发范围清单。

审核报告经管理者代表批准后发放，原件由安全管理小组存档，作为管理评审输入的一部分。审核完成后要对内审结果进行整理与分析。

纠正预防措施预定日期已到或接到完成通知时，银行的信息安全审计组长应指派审计人员到受审计方验证其纠正预防措施完成情况，验证有效后，信息安全审计组长应在《纠正预防措施表》的“整改结果验证评估”栏中签字。

信息安全审计报告及相应的审计证据、审计发现的纠正预防措施表及跟踪验证的审计资料，作为银行内部重要且敏感的信息资产应妥善保管。

审核中发现有不符合项的责任部门，应立即将发现的不良现象控制或消除、调查分析产生问题的原因、评价确保不合格不再发生的措施的需求、针对原因提出纠正预防措施、彻底付诸实施并控制纠正预防措施的执行情况、记录所采取的纠正措施的结果。

负责跟踪验证的内审员应协助责任部门纠正措施的制定与实施，评审所采取的纠正措施的效果，具体包括：

1）评价措施是否针对提出的不符合项进行，若有其他问题也应指出。

2）原因是否彻底分析清楚，是否抓住要害。

3）实施过程中有无困难，是否需要配合和支持。

4）涉及文件更改、体系调整的是否有效执行。

5）是否在要求的时限内完成。

6）重新抽样验证的最终效果如何。

7）有无必要的记录，记录控制得如何。

在“不符合项报告”规定的期限内，跟踪人员要对不合格项目进行跟踪验证和报告，有纠正措施且可以防止同类问题再次发生的，则可“关闭”。当责任部门不能按时有效提供纠改预防措施时，可升级问题。

所有的内审计划、通知、记录、报告等，都应妥善归档于安全管理小组或审查项目组织部门，纠正和预防措施的跟踪验证报告应作为管理评审输入的一部分。

第三篇

技术篇

除信息安全管理外，信息安全技术同样是保证银行信息系统安全不可或缺的部分。信息安全技术主要通过在信息系统中部署合适的软硬件，并正确配置其安全功能来实现。本篇将讲述保障银行信息系统安全的相关技术。

第 13 章
信息安全技术模型

信息安全模型在信息系统安全建设中起着重要的指导作用，可以精确而形象地描述信息系统的安全属性，准确地描述安全的重要方面与系统行为的关系，能够提高成功实现关键安全需求的理解层次，并且能够从中开发出一套安全性评估准则和关键的描述变量。而信息安全技术模型是信息安全模型的子集，一个好的信息安全模型必然带有一个好的信息安全技术模型。

ISO/OSI 安全体系为信息安全问题的解决提供了一种可行的方法，但其操作性方面与实际情况还有一定差距，特别是在表现技术实现上，对实际工作的指导意义还不够。

在信息安全工作中，一般采用 PDR（保护、检测和响应）、PPDR（安全策略、保护、检测和响应）、PDRR（保护、检测、响应和恢复）、MPDRR（管理、保护、检测、响应和恢复）和 WPDRRC 等动态可适应安全模型，来指导信息安全实践活动。

考虑到对中国国情的适应性和中国银行业对信息安全的高度重视，信息安全的投入相对有保障等因素，本书将以 WPDRRC 模型为基础，构建信息安全技术的层次技术模型。

13.1 WPDRRC 介绍

WPDRRC 模型是我国“八六三”信息安全专家组提出的适合中国国情的信息系统安全保障体系建设模型，它在 PDRR 模型的前后增加了预警和反击功能，有六个环节和三大要素。六个环节包括预警、保护、检测、响应、恢复和反击，它们具有较强的时序性和动态性，能够较好地反映出信息系统安全保障体系的预警能力、保护能力、检测能力、响应能力、恢复能力和反击能力。三大要素包括人员、策略和技术，人员是核心，策略是桥梁，技术是保证，落实在 WPDRRC 六个环节的各个方面，将安全策略变为安全现实。WPDRRC 模型的结构如图 13-1 所示。

WPDRRC 模型在实际工作中发挥着日益重要的作用，它所包含的六个环节，其内

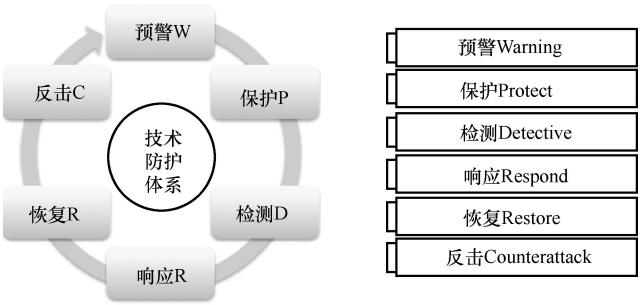


图 13-1　WPDRRC 模型

容如下：

1）预警：通过检测等手段，事先掌握系统的脆弱性，了解当前环境的各种威胁和犯罪趋势，预测未来可能受到的攻击，以及可能承受的损失。

2）保护：指采取各种手段，来防护信息安全系统，阻止可以发生攻击的条件的产生，让攻击者无法顺利地入侵信息系统，以此来减少大多数的入侵事件。

3）检测：利用各种技术手段和工具，检测系统中是否存在黑客攻击或者其他可能影响系统安全的威胁因素，包括可能被攻击者利用的黑客工具、病毒、各种漏洞等。

4）响应：通过综合手段建立起来的快速响应机制，如报警、跟踪、处理（封堵、隔离、报告）等，实时阻止已经发生或即将发生的攻击行为，避免或者减少攻击行为造成的实际伤害。

5）恢复：对所有数据进行备份，并采用容错、冗余、替换、修复和一致性等手段，保证信息系统受到冲击时，能迅速恢复正常运转。

6）反击：具备一定取证手段，利用各种技术手段和工具，去发现攻击的线索和证据，并向有关机构提供相关信息和依据；具备一定打击手段，在法律框架内，依法打击犯罪和网络恐怖分子。

13.2　安全技术的层次结构模型

安全技术对信息系统的保护不仅体现在 WPDRRC 的各个环节中，还体现在直接保护对象的差异上，它体现了不同层次的需求。

按照中国等级保护体系的要求，可以将技术要求分为物理安全、网络安全、主机安全、应用安全和数据安全等五个层面，其层级结构模型如图 13-2 所示。

1）物理安全：是指为了保证信息系统安全可靠地运行，确保信息系统在对信息进行采集、处理、传输、存储过程中，不至于受到人为或自然因素的危害，而使信息丢失、泄露或被破坏，对计算机设备、设施（包括机房建筑、供电、空调等）、环境人员、系统等采取适当的安全措施。

2）网络安全：是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受破坏、更改、泄露，系统能连续可靠正常地运行，网络服务不中断。从而确保网络数据和通信的可用性、完整性和保密性。

3）主机安全：是指通过各种手段，保证主机在数据存储和处理时的保密性、完整性、可用性，它包括硬件、固件、系统软件的自身安全，以及一系列附加的安全技术和安全管理措施，从而建立一个完整的主机安全保护环境。

4）应用安全：就是保障应用程序使用过程和结果的安全，是针对应用程序或工具在使用过程中可能出现的计算、传输数据的泄露和失窃，通过各种安全工具和手段来消除隐患。

5）数据安全：通过采用各种手段，使信息系统正常运行，从而确保所有数据的可用性、完整性和保密性；数据安全还包括备份和恢复等内容，保证信息系统在遭受巨大冲击时，可以及时地恢复数据，恢复正常运行。

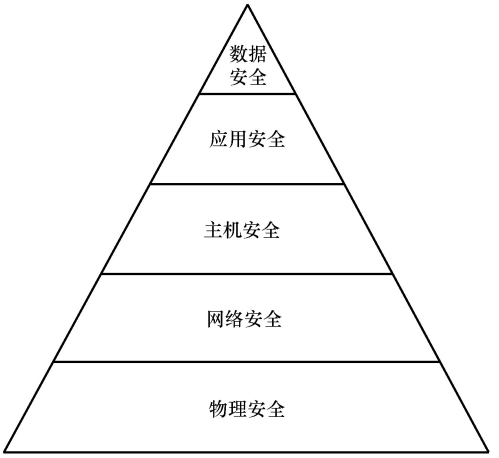


图 13-2　安全技术层级结构模型

13.3　基于 WPDRRC 的层次技术模型

安全技术手段，一方面在 WPDRRC 模型的预警、保护、检测、响应、恢复和反击六个环节中分别发挥作用；另一方面，从安全技术的保护对象和层次来看，又可以在物理安全、网络安全、主机安全、应用安全和数据安全等五个层面发挥作用。两个维度结合，就能精确地描述出安全技术在整个信息安全中的作用。

在银行业，信息安全保障的高要求导致大量的安全技术被采用，常用的信息安全技术手段与 WPDRRC 层次模型的对应关系见表 13-1。

后面将按照物理安全、网络安全、主机安全、应用安全、数据安全五个层面展开描述，其中的密码技术和安全工具、安全检测与渗透测试、安全运营技术、灾难备份与恢

复部分内容涉及多个层面，且内容比较多，也以独立章节的形式做了描述。

表 13-1　常用的信息安全技术手段与 WPDRRC 层次模型的对照

	预防	保护	检测	响应	恢复	反击
物理层	门禁 物理区域隔离	门禁 UPS 防火设备 防水设备	视频监控 烟雾探测	视频监控	容灾中心	（无）
网络层	漏洞扫描系统 VLAN 技术 安全域划分与控制 无线网络安全技术 设备补丁管理	入侵保护 防火墙 VPN WEB 应用防火墙 DDoS 防御网关 网络准入系统 防病毒网关	入侵检测 IDS 入侵防御 IPS 异常流量监管系统 网络日志审计 渗透测试	异常流量监管 网络安全运维	网络备份与恢复 双链路 双机热备	IP 地址反追踪 流量干扰 证据采集
主机层（含终端）	漏洞扫描系统 系统补丁管理 安全加固	入侵保护 病毒防护 防篡改系统 WEB 应用防火墙 身份鉴别 访问控制	病毒防护 主机系统审计 数据库审计 渗透测试 网站综合监控 4A 平台	病毒防护 应急响应技术	系统备份与恢复 双机热备 服务器集群	证据采集
	终端安全管理技术 网络准入	终端安全管理技术 存储介质保护 数据防泄漏 防病毒系统	数据防泄漏 防病毒系统	防病毒系统 应急响应技术	（无）	
应用层	渗透测试 源代码安全 检查技术 安全开发	入侵保护 WEB 应用防火墙 安保平台 身份鉴别 访问控制	应用漏洞扫描 应用日志审计 渗透测试	应急响应技术	负载均衡	权限控制 反钓鱼技术 证据采集
数据层	数据加密管理技术	数据脱敏	网络及主机审计技术适用	应急响应技术	数据备份与恢复	证据采集

第 14 章
物理安全

物理安全保护的目的主要是使存放计算机、网络设备的机房及信息系统的设备和存放数据的介质等免受物理环境、自然灾害，以及人为的误操作和恶意操作等各种威胁所产生的风险。物理安全是防护信息系统的最底层，缺乏物理安全，其他任何安全措施都将变得毫无意义，因此物理安全是银行信息安全建设的重要内容。本章介绍了物理安全的基本概念、物理安全要素及物理安全的要求与内容。

14.1 物理安全概述

物理安全是指为了保证信息系统安全可靠地运行，确保信息系统在对信息进行采集、处理、传输、存储的过程中，不至于受到人为或自然因素的危害，而使信息丢失、泄露或被破坏，对计算机设备、设施（包括机房建筑、供电、空调等）、环境人员、系统等采取适当的安全措施。物理安全的直接保护对象是硬设备，硬设备的安全是信息系统安全的基础。

物理安全通常包括计算机机房（数据中心）及办公环境的物理安全。

14.2 物理安全要素

14.2.1 物理资产分类

物理资产指信息系统中的各种硬件、软件和物理设施，其通常的分类方式有：

1）计算机设备：各种服务器、桌面计算机、笔记本电脑等。

2）通信设备：路由器、交换机、防火墙等。

3）技术设备：电源、不间断电源（UPS）、空调等。
4）存储介质：光盘、U 盘、磁带等。
5）家具及固定装置：机柜、机架等。
6）其他。

14.2.2 物理安全威胁

信息系统物理安全面临多种威胁，既可能面临自然、环境和技术故障等非人为因素的威胁，也可能面临人员失误和恶意攻击等人为因素的威胁，这些威胁通过破坏信息系统的保密性（如电磁泄漏类威胁）、完整性（如各种自然灾难类威胁）、可用性（如技术故障类威胁）进而威胁信息的安全。造成威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种；环境因素包括自然界不可抗的因素和其他物理因素。表 14-1 对物理安全威胁的种类进行了描述。

表 14-1 物理安全威胁种类清单

种类	描　　述
自然灾害	鼠蚁虫害、洪灾、火灾、地震等
电、磁环境影响	断电、电压波动、静电、电磁干扰等
物理环境影响	灰尘、潮湿、温度等
软硬件故障	由于设备硬件故障、通信链路中断、系统本身或软件缺陷对信息系统安全造成的影响
物理攻击	物理接触、物理破坏、盗窃
无作为或操作失误	由于应该执行而没有执行相应的操作，或无意地执行了错误的操作，对信息系统造成的影响
管理不到位	物理安全管理无法落实或不到位，造成物理安全管理不规范，或者管理混乱，从而破坏环境信息系统，使其正常有序地运行
恶意代码和病毒	改变物理设备的配置，甚至破坏设备硬件电路，致使物理设备失效或损坏
网络攻击	利用工具和技术，如拒绝服务等手段，非法占用系统资源，降低信息系统可用性
越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的职权，做出破坏信息系统的行为，如非法设备接入、设备非法外联
设计、配置缺陷	设计阶段出现明显的系统可用性漏洞、系统未能正确有效配置、系统扩容和调整引起的错误

14.2.3 物理安全脆弱性

脆弱性是信息系统本身存在的，威胁总是要利用信息系统的脆弱性造成危害。物理设备安全的脆弱性可以从以下方面进行识别：防电磁信息泄露、抗电磁干扰、电源保护及设备振动、碰撞、冲击适应性等；物理环境安全的脆弱性可以从以下方面进行识别：机房场地选择、机房屏蔽、防火、防水、防雷、防鼠、防盗防毁、供配电系统、空调系统、综合布线、区域防护等；系统自身物理安全的脆弱性可以从以下方面进行识别：灾

难备份与恢复、边界保护、设备管理、资源利用等。

14.3 物理安全的要求及内容

物理安全保护的要求是复杂的，其基本要求包括：

1）物理位置的安全，包括机房和办公场地的位置。

2）物理访问的控制。

3）防盗窃和防破坏。

4）防雷击。

5）防火。

6）防水、防潮。

7）防静电。

8）温湿度控制。

9）电力供应。

10）电磁防护。

上述要求对于银行数据中心和办公环境均适合。考虑到叙述的简洁性，以下主要从数据中心的角度进行说明。

14.3.1 物理位置的选择

对于银行这样的企业数据中心运行着的银行生产系统，为确保数据的安全，数据中心的选址是至关重要的，即必须在交通、通信便捷的地区，而且具有防震、防风、防雨等能力的建筑内。

在多层建筑或高层建筑物内的机房，宜设于第二至五层，不宜设在一层或顶层。

计算机系统受粉尘、有害气体、震动冲击、电磁场干扰等因素的影响会导致运算差错、误动作和机械部件磨损，缩短计算机使用寿命。因此机房位置应尽可能选择远离产生粉尘、有害气体、强震源、强噪声源等场所，避开强电磁场干扰。对强电磁场干扰这一因素，必要时需做实地测量来确定。

14.3.2 物理访问的控制

银行需要建立机房安全管理制度，对进出机房的人员进行控制、鉴别和记录，同时对进入机房的来访人员采取申请审批，并在进入机房后进行监控和限制其活动范围。对银行机房的物理访问控制包括以下八个方面：

1）出入机房区域的所有人员须佩戴机房出入证，无证者不能进入。

2）机房工作人员及需要长期进入机房区域工作的人员，在得到机房相关部门授权

后，使用固定期限出入证出入。

3）外来人员（包括厂家工程师、参观者及其他外访人员）进入机房区域须事先预约登记，并由相关人员陪同，在批准有效期内持临时出入证出入。

4）除授权人员外，任何进入机房区域的人员须履行登记手续，按规定填写《机房出入登记表》。具体格式参见表 14-2。

5）只有与卡号登记相符的持卡人员才可以使用机房门禁卡，各持卡人未经机房管理人员同意，不得将门禁卡转借他人。

6）人员进入机房，禁止携带可能影响和威胁机房正常运行的物品，如食品和饮料，香烟，易燃易爆物品，电磁设备，放射性物品，以及任何照相机和录音器材等。

7）计算机等设备的出入须遵守机房移入移出设备管理规定，履行设备移入、移出的申请和登记流程。

8）进入机房区域的人员须遵守关于机房的各项规章制度。

表 14-2　机房出入登记表

姓名	单位	进入机房事由	进入机房 授权人员签字	进入(日期/时间)	离开(日期/时间)

14.3.3　防盗窃和防破坏

银行应将主要设备放置在机房内，对机房的所有资产进行介质分类标识，形成档案或介质库进行保存。对于机房的通信线缆，应将其铺设在地下或管道中进行隐藏以免遭到破坏。

建立机房设施与环境监控系统，对机房空调、消防、不间断电源（UPS）、供配电、门禁系统等重要设施实行全面监控。

对机房环境一般实行 7×24 小时集中综合监控。运行监测岗位的人员实时监控电源系统、空调系统和机房环境，定期巡检、维护场地设施，填写巡检日志，记录、处理和报告监控系统终端各种声、光告警模块发出的报警信息。

14.3.4　防雷击

随着金融电子化建设步伐的不断加快，电子设备被广泛应用于金融网络的运行系统中。这些高精密的电子计算设备富含大量的 CMOS 半导体集成模块，普遍存在着绝缘强

度低、过电压耐受能力差等致命弱点，一旦遭受雷击过压的冲击，会造成这些电子系统的运行中断，设备永久性损坏；重要的是这些系统所承负的那些须实时运行的后续工作的中断瘫痪所造成的不可估量的直接与间接的巨大经济损失和影响。对雷电电磁脉冲（LEMP）的防护，不但是必要的，而且是必须实施的。随着电子设备的广泛应用，雷击设备事故概率的增加及人们防雷意识的增强，日趋显示了电涌保护器（防雷器，简称 SPD）在保障电子设备的运行安全性方面起到的作用和地位。

根据 GB 50057—2010《建筑物防雷设计规范》中规定，银行应为第二类防雷建筑物，并应按第二类防雷建筑物采取相应的防雷措施；第二类防雷建筑物防直击雷的措施，宜采用装设在建筑物上的避雷网（带）或避雷针或由其混合组成的接闪器。

防雷工程分为直击雷和雷电感应两大部分。直击雷防御系统的主要作用，是捕捉雷电闪击点，保护建筑物及室外部分设备免受雷电的直接打击。直击雷防御系统的主要组成部分为接闪器（避雷针、带、网）、引下线、接地装置。雷电感应防御系统的主要作用，是降低雷击时的冲击电位差和雷电电磁感应强度，保护电子设备免受雷击过电压和雷电电磁脉冲的危害。雷电感应防御系统的主要组成部分为电磁屏蔽、电涌保护器、等电位连接。在防雷工程设计时应系统地、因地制宜地将直击雷防御和雷电感应防御有机地结合起来，才能保证整体防雷工程的有效性，因此整体防雷工程应从以下几个要素着手。

1）捕捉雷电闪击。在大楼顶部安装接闪器，让雷电按指定的途径泄放入地，避免微波接收天线等直接接受雷电流而受损。

2）雷电流的安全输送。利用引下线引导强大的雷电流安全入地。

3）雷电能量的对地安全释放。利用良好的接地网系统尽快地泄放雷电能量。降低雷电流的落地电位差，尽可能降低地电位反击能量。

4）雷电电磁波的屏蔽。利用建筑物的钢筋混凝土墙体、专用屏蔽罩及各种设备自身的金属屏蔽层，衰减雷电电磁脉冲产生的强大磁场对设备中的电子芯片的电磁危害。

5）防止雷电波通过电力线缆、通信线缆、天馈线缆及其他金属线缆对设备造成的过电压损害。利用相应的电涌保护器，在线路的入口处进行雷电能量拦截，使到达设备的雷电过电压在设备可承受的范围之内。

6）防止不同地网及相邻金属导体之间产生电位差。采用共地、等电位连接、地网均压等措施，防止雷击电位差对设备的危害。

14.3.5 防火

银行数据中心机房 IT 系统的正常运行至关重要，系统运行和核心数据的存储关系到银行乃至社会的命脉，必须对这些重要的设备设计好消防系统，防患于未然。

1. 火的种类

火分为以下几类：

A 类——固体有机物质燃烧的火；

B 类——液体或可融化固体燃烧的火；

C 类——可燃气体燃烧的火；

D 类——轻金属燃烧的火。

2. 灭火原理及介质

常见的灭火器有干粉类的灭火器、二氧化碳灭火器、泡沫型灭火器、水型灭火器等，其灭火原理各不相同，通常包括：

（1）冷却法 将灭火剂直接喷到燃烧物上，使燃烧物质的温度降低到燃点之下，而停止燃烧。

（2）隔离法 将火源处及其周围的可燃物撤离或隔开，使燃烧因与可燃物隔离而停止。

（3）窒息法 阻止空气流入燃烧区或用不燃烧物质冲淡空气，使燃烧物质得不到足够的氧气而熄灭。

（4）中断化学反应法 灭火剂参与到燃烧反应过程中，使燃烧过程产生的游离基消失，而形成稳定分子或活性的游离基，从而使燃烧的化学反应中断。

不同类别的火源，其对应的灭火介质有所区别，具体参见表 14-3。

表 14-3 不同等级防火对应的灭火介质

等级	类型	灭火介质
A	普通可燃物	水、苏打酸
B	液体	气体、CO_2、苏打酸
C	气体	气体、CO_2
D	可燃金属	干粉

银行数据中心灭火系统禁止采用喷水、泡沫及粉末灭火，比较适合用气体灭火系统。数据中心的消防系统应该是相对独立的系统，一般在大型的数据中心中都具备集中监控系统，系统可以准确预报火警，并且在无人值守的情况下自动启动消防灭火系统。

3. 银行防火考虑要点

1）为预防来自机房外部的火灾危险，理想的情况下机房最好与其他建筑分开建设，并在建筑之间留有一定宽度的防火通道。如果机房与其他用途的房间合用一幢建筑，根据建筑设计防火规范及机房设计规范规定，应单独设防火分区。这样可以有效地防止来自机房外部的火灾危险。在机房选址时应注意机房要远离易燃易爆物存放区域。

2）机房应为独立的防火分区，机房的外墙应采用非燃烧材料。进出机房区域的门应采用防火门或防火卷帘。穿越防火墙的送、回风管，应设防火阀。以上措施应在机房平面总体设计及相关专业设计中同步进行。

3）机房建设采用防火材料。机房内部的建筑材料应选用非燃烧材料（A 级）或难燃烧材料（B 级）。

4）设置火灾报警系统。在数据中心设置消防信道并放置对计算机影响较小的气体灭火设备，同时建立火灾自动报警系统。对于灭火设备的摆放位置和有效期进行不定期

检查，确保灭火设备的可用性。

5）设置气体灭火系统。

6）合理正确使用用电设备，制定完善的防火制度。

14.3.6 防水和防潮

1. 防水

数据中心的房顶不允许有水管穿过，如果水管在地板穿过，则必须采取相应的保护防范措施。在机房的窗户、屋顶、墙壁设置保护措施以防止雨水的渗透。对于湿度较高的地区或季节应做好防潮处理。

为防止空调系统漏水对机房产生的灾难性后果，须在精密空调周边安装防水坝并配备漏水检测系统和排水装置。

2. 防静电

在数据中心安装防静电地板，进入机房的作业人员必须配备防静电手套。

（1）静电防护的基本原则

1）抑制或减少机房内静电荷的产生，严格控制静电源。

2）安全、可靠、及时地消除机房内产生的静电荷，避免静电荷积累。静电导电材料和静电耗散材料用泄漏法，使静电荷在一定时间内通过一定的路径泄漏到地。

3）绝缘材料用以离子静电消除器为代表的中和法，使物体上积累的静电荷吸引从空气中来的异性电荷，被中和而消除。

4）定期（如一周）对防静电设施进行维护和检验。

（2）静电电压 静电电压绝对值应小于200V

（3）地面要求

1）当采用地板下布线方式时，可铺设防静电活动地板。

2）当采用架空布线方式时，应采用静电耗散材料作为铺垫材料。

（4）其他防静电措施

1）必要时装设离子静电消除器，以消除绝缘材料上的静电和降低机房内的静电电压。

2）垫套、手套均应为防静电的。

3. 温、湿度控制

在数据中心设置温、湿度自动调节设施，使机房温度、湿度的变化在设备运行所允许的正常范围内，并监控温、湿度自动调节设备的工作状态，在超出允许范围后自动发出警告给工作人员。

活动地板铺设在计算机机房的地面找平层上，在活动地板与建筑地面之间的空间内可以铺设连接设备的各种管线。活动地板下空间可作为静压送风风库，通过带气流分布风口的活动地板将机房空调冷风送入室内及发热设备机柜内，机房内能自由调节气流

分布。

活动地板下的空间作为静压送风风库，送风温度约为 14℃，将与下层天花产生极大温差，容易在下层天花产生冷凝水。机房、电池室地板下需铺设橡塑保温板，所有接缝应整齐贴紧，达到良好的保温、节能效果，并具有足够的强度来抵御磨损，橡塑保温面层铺设镀锌钢板。

14.3.7 电力供应

银行机房电气工程中的机房供配电系统是数据中心机房的生命线，因此要建一个好的机房，首先要将供配电解决好。一般要求主要开关设备应该被设计成适合增容、维护和冗余，并提供双倍的或隔离的冗余配置。设计时应该考虑到开关装置、总线或断路器维护的方便性。瞬时电压浪涌抑制（TVSS）应该被安装在电力分配系统的每一级上，并且采用适当的规格，以便能够抑制可能发生的瞬时的能量。

同时，为保证机房设备正常运转，在数据中心的供电线路上应配备稳压器和过电压防护设备；在机房出现断电的情况下为保证设备正常运转，机房还配备了短期的备用电力（发电机、蓄电池）来提供超过 1 小时的供电时间，在机房的特殊区域和重要设备要单独提供 UPS 来供电。

对于一级负荷机房应该有从不同变电站供给的双路供电，加上柴油发电机，通过应急电源柜切换后供给机房内的 UPS 和精密空调机组，ATS 切换最好在机房配电系统就近设计，切换后以最短距离输送给机房设备。备用发电机系统是至关重要的一个因素。即便其中有一个故障，也能够直接地向计算机和其他设备提供一个理想质量和容量的电力供应。发电机的设计应能够处理 UPS 系统或计算机设备负荷的谐波电流。备用发电机应该提供备用电源给所有的冷却设备，避免负载设备温度上升及停止运行。如果发电机不支持这些系统，它们所带来的益处就显得很有限。在自动控制发生故障时，发电机应该能够采用手动控制。应该给每一个发电机输出提供瞬时电压浪涌抑制装置。

配电必须充分考虑到今后的发展余量。如一台服务器，每台高配功率为 1kW，一个机柜若装 6 台就是 6kW，假如预期机房在今后会装到最多 40 个机柜那就是 240kW；UPS 一般可按照设备容量的 1.3 倍计算，就是 312kVA，再加上适当的余量，选用 3 台 200kVA UPS 冗余供电是一种较为理想的方案。

14.3.8 电磁防护

电源线和通信线路应隔离铺设，避免互相干扰从而影响数据中心的正常运作。

主机房内无线电干扰场强，在频率为 0.15～1000MHz 时，不应大于 126dB。

在计算机系统停机条件下，主机地板表面垂直及水平向的振动加速度值不应大于 500mm/s^2。

主机房内磁场干扰环境场强不应大于 800A/m。

主机房地面及工作台面的静电泄漏电阻，应符合现行国家标准 SJ/T 10796—2001《计算机机房用抗静电活动地板技术条件》的规定。

主机房内绝缘体的静电电位不应大于 1kV。

14.4 案例介绍：物理安全建设实例

某商业银行 A 分行数据中心机房是其分行数据信息交换的中心，按照计算机机房和通信机房的标准设计，拟在其新的办公基地一、二层新建数据中心机房，满足 A 分行今后五年的发展需要。建成后，该机房将成为 A 分行业务数据储存及交换的核心基地，因此对该机房的建设提出了更高的物理安全要求。

根据 A 分行建设要求，其新数据中心机房物理安全包括以下内容：

1）机房应具有抵御自然灾害如地震、水灾、火灾、鼠虫害等的能力，以及防火、防雷、防水、防静电等能力，定期检查并适当测试以确保上述功能的有效性，减少由于故障或失效带来的风险。

2）机房出入口应有专人值守，进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

3）机房应划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域。

4）设备或主要部件应设置明显的标记，利用光、电等技术设置机房的防盗报警和监控报警系统。

5）机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

6）应在机房供电线路上设置稳压器和过电压防护设备，提供备用供电系统和冗余电力线路，满足主要设备在断电情况下的正常运行要求。

7）应采用接地方式防止外界电磁干扰和耦合干扰，电源线和通信线缆应隔离铺设，避免互相干扰，并对关键设备和磁介质实施电磁屏蔽。

为满足上述建设内容，该分行新数据中心机房的物理安全按照 GB 50462—2008《电子信息系统机房施工及验收规范》定义的“A 类机房标准”要求和《A 商业银行机房建设规范》等标准进行设计。机房建设工程的主要内容如下。

1. 装修及承重

装修是整个机房的基础，它主要起着功能区划分及保证机房环境的作用。主要内容包括以下几个方面。

1）隔断处理：机房外围隔断采用轻质隔断，机房内部隔断采用防火玻璃隔断或彩钢板隔断。

2）墙面处理：机房四周采用彩钢板装修及乳胶漆面，柴油发电机房做隔音。

3）天面处理：所有机房天面都刷防尘防潮漆，有设备区域还要贴保温棉，其他区

域安装铝扣板天花。

4）地面处理：所有机房地面都刷防尘防潮漆，空调区、配电区及信息技术设备区域需贴保温棉，并架高 500mm 的防静电地板，其中维修间、气瓶间、油机间地面贴地砖。

5）门体处理：机房内所有门体都采用防火门，防火门均应采用消防局认可的合格产品。

6）承重支架：空调间、UPS 间及电池间所有设备均不能直接落地安装，都要安装有承重支架。

2. 机柜及 PDU

机柜承载着机房的核心设备，其主要包括以下几个方面。

1）服务器机柜：配置 39 套服务器机柜（600mm × 1070mm × 2070mm），网孔门。

2）网络机柜：配置 18 + 10 套网络机柜（800mm × 960mm × 2070mm），网孔门。

3）接入机柜：配置 10 套电信机柜（600mm × 600mm × 2070mm），网孔门。

4）机柜 PDU：每个机柜配 2 个 PDU。

5）机柜顶部走线系统：每个机柜都配置强弱电线槽模块。

3. 供配电系统

需求测算：已知目前机房信息技术负载约 40kW，考虑到未来扩容需要，新建机房按满载 80kW 规划设计。

供配电系统是机房安全高可用性的基础和保障机房安全运行的关键。机房工程供配电系统采用三相五线制一类供电，采用 2N 模式的供电接线方式，分别从大楼负一楼的不同市电切换柜引 2 路市电、1 路油机，通过强电井引入 UPS 配电间，再经过 ATS 切换给机房的设备供电。

根据前面的电力测算：要求大楼提供双路市电，容量为 630A，配置的柴油发电机组常用功率约 460kW。

设计内容主要包括：

1）油机内容：配置一套柴油发电机组，安装在负一楼，功率约 460kW。

2）配电柜：在五楼机房配置 ATS 双电源切换、UPS 输入配电柜、UPS 输出配电柜、市电配电箱等。

3）强电电缆：内容包括机房的主输入电缆及机房内部的强电电缆。

4）防雷接地：配置电源防雷器系统及机房内的等电位连接。

5）照明系统：机房内配置节能照明系统及应急照明系统。

6）机架式 STS 电源：共配置 6 个 STS 电源模块。

4. UPS 供电系统

UPS 电源设备是机房供配电系统中的核心设备，同时它也是关系到整个数据中心 PUE 值的关键性指标。UPS 电源系统包括：

1）核心机房：UPS 供电模式采用 2（1 + 1）系统，配置 4 台 UPS 主机，单台功率为 120kVA。

2）楼层其他业务：利用现有的 2 台 80kVA 的 UPS 主机，通过（1 + 1）并机冗余方

式对营业部、保卫部的监控室、楼层机房总体供电。

3）华南处理中心：配置 1 台 30kVA 的 UPS 主机，主要是负责华南处理中心的供电。

4）后备电池：每台 UPS 主机按后备 1 小时时间来配置电池组。

5. 精密空调系统

精密空调与气流组织是机房运行环境的保障，是为数据中心机房提供合适的温度、湿度和洁净度的决定性条件。

通过计算得出数据分析：机房满载运行时，需最大的制冷量为 150kW，机房共规划 5 台风冷型精密空调，采用（3 +2）冗余制冷模式，给机房的信息技术设备及电源设备提供冷量，其中利用现有的 3 台精密空调，单台制冷量为 57kW，新增 2 台精密空调，单台制冷功率为 42kW。

精密空调系统包括冷气流产生单元、气流配送单元和气流回收单元。

1）精密空调设备（冷气流产生单元）：共 4 台精密空调。

2）出风地板（冷气流配送单元）：采用地板下送风上回风方式。

3）气流遏制子系统（热气流回收单元）：通过自然回风方式。

4）配置完善的管道系统及给排水系统。

另外操作间及休息间配置舒适空调（2 台 2P 的天花机及 1 台 1P 的壁挂机）。

6. 新风系统

新风系统是降低数据中心机房空调系统能耗的一个重要的辅助措施，也是保证机房正压的唯一手段。新风系统为机房工作人员提供必要的新鲜空气，是降低机房能源消耗的重要手段。主要包括：

1）新风机：机房配置一套新风机系统。

2）排风机：机房配置一套排风机系统。

3）管道：配置完善的管道系统。

7. 综合布线系统

本项目综合布线系统工程采用 6 类布线产品，能具备语言、数据、图像、监控系统中信号传输的要求，类型为综合型，为开放式结构，容易扩展、变更，包括网络布线、控制及其他可能应用的智能化系统。

1）主要分布区域（MDA）：网络设备区，用于安装网络设备、核心交换机、外联设备等，网络结构采用一主一备，是数据中心结构电缆系统分布区域的中心点。

2）水平分布区域（HAD）：网络列头柜区，主要用于由每列服务器机柜引来的线缆及核心配线柜引来的骨干缆成端配线架，同时安装诸如 LAN 和位于设备分布区域末端设备的 KVM 等设备。

3）设备分布区域（EDA）：服务器机柜用于安装服务器、存储设备等，并成端由列头柜引来网络线。

4）机房布线采用 6 类非屏蔽布线系统和万兆多模光纤布线系统。

5）综合布线系统采用机柜上走线方式。

8. 综合监控系统

机房综合监控系统是机房智慧化管理的一个重要手段。机房控制应具有高度自动化，它要求以最少的维护人员，最优化的运营维护手段，来实时监控每一个机房中设备所处的物理环境。同时，集成安防系统的各个子系统，使管理高度集中化、智能化，优化资源分配。机房综合监控系统主要包含以下几个方面。

1）设备监控子系统（配电柜、UPS 主机、电池组）。

2）环境监控子系统（温湿度、漏水、烟感）。

3）消防联动与控制子系统。

4）资产管理子系统。

5）能源监测与管理子系统。

6）故障报警系统（声光、短信、邮件、IE）。

9. KVM 设备管理系统

KVM 设备管理系统是现代计算机机房的集中控制管理机房内计算机设备的一个科学先进的工具。通过高质量的数字式的 KVM（键盘、鼠标和显示器）切换器及相关的连接产品，可实现在本地及远程可远距离集中控制管理操作机房内的各小型机系统、PC 服务器及网络设备。它包括以下几个方面。

1）KVM 切换主机：共配置 3 台 32 口的数字 KVM 主机。

2）模块：每个 KVM 配置 32 个转换模块，共 96 个。

3）网络布线：KVM 布线采用超 5 类布线方式。

10. 气体消防系统

气体消防系统是整体机房安全运行的盾牌。从对火警的探测系统来看，它具有温感、烟感探测器，红外探头；对于灭火系统来说，基本上大多数机房都采用的是气体灭火系统。这就要求在整体机房的设计和施工中，必须规划、建设钢瓶间、消防控制间和一些管道（也可使用无管网系统），从而达到全方位报警、分区灭火，最大限度地提高对火灾的防范能力。其内容包括：

◇ 气体灭火装置。

◇ 消防控制子系统。

◇ 消防管道子系统。

◇ 消防排烟子系统。

◇ 消防联动子系统。

11. 门禁系统

为了保证对机房区域进行有效的人员管理，在机房出入口及各功能区域入口均设置门禁系统。各功能区域入口和机房主入口人员的管理权限逐级递减，满足重要设备间与普通操作间分区管理的目的，避免了由于人员管理模糊所产生的隐患。门禁系统设置两套，分别安装在一、二层机房，各系统自带有通信模块，可通过网线并入大楼以太网（Ethernet），方便远程用户的检测。

第 15 章
网络安全

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断，从而确保网络数据和通信的可用性、完整性和保密性。网络安全保护的对象是网络系统的硬件、软件。对于银行信息系统来说，网络安全保护对信息系统的访问、读写等操作进行保护和控制，数据传输受到保护，避免出现病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。由此可见，网络安全技术涉及面非常广。本章主要对网络安全的常见技术进行了介绍，包括防火墙技术、入侵检测/保护技术、VPN 技术、无线安全技术及网络设备安全防护等内容。

15.1 典型的银行网络安全设计示例

典型的银行网络安全设计拓扑图如图 15-1 所示。在建设规划时采用分层、分区的规划思路，通过部署防火墙、IDS、IPS、VPN、负载均衡、DDoS 防护等安全设备来保障网银系统的安全。后面将对防火墙、IDS、IPS、VPN 等安全设备做详细的介绍。

15.2 防火墙技术

15.2.1 防火墙概述

防火墙这个词来源于建筑词汇，用于限制（潜在的）火灾在建筑内部的蔓延，后被引申至信息安全领域中访问控制、边界整合类的产品，防火墙是一种访问控制技术，在某个机构的网络和不安全的网络之间设置障碍，阻止对信息资源的非法访问。

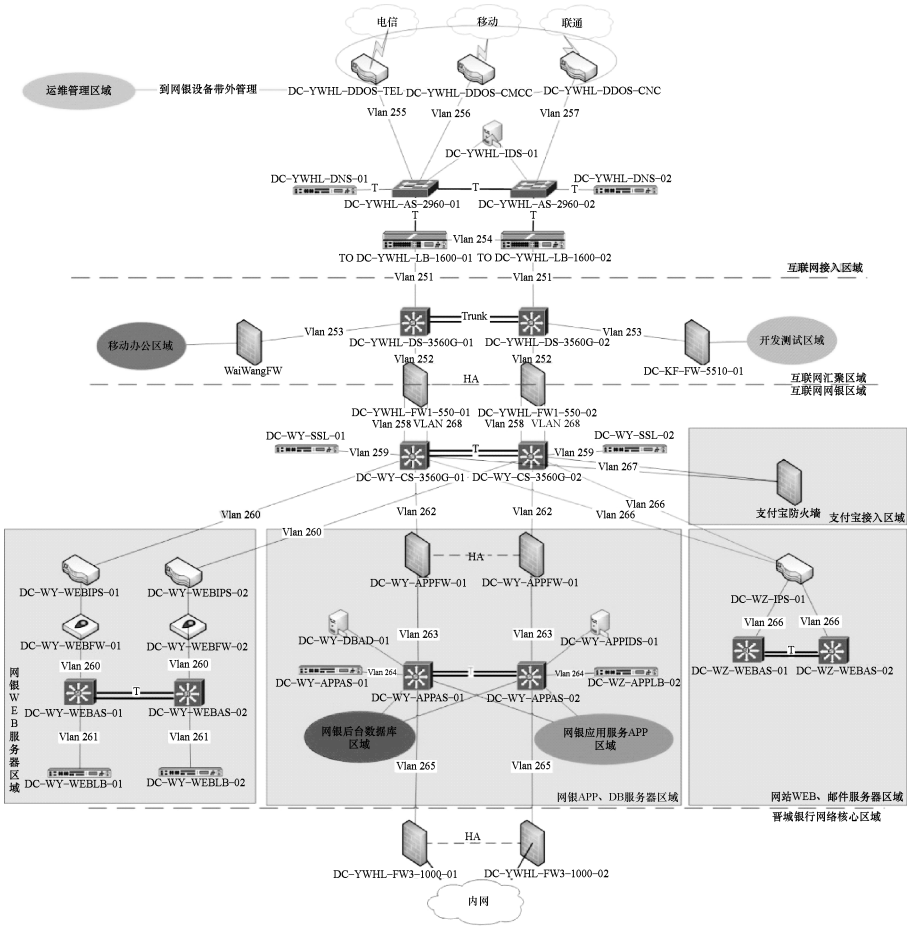


图 15-1　典型的银行网络安全设计拓扑图

Internet 的发展给政府结构、企事业单位带来了革命性的改革和开放。他们正努力通过利用 Internet 来提高办事效率和市场反应速度，以便更具竞争力。通过 Internet，企业可以从异地取回重要数据，同时又要面对 Internet 开放带来的数据安全的新挑战和新危险，即客户、销售商、移动用户、异地员工和内部员工的安全访问；以及保护企业的机密信息不受黑客和工业间谍的入侵。因此企业必须加筑安全的“战壕”，而这个“战壕”就是防火墙。防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，越来越多地应用于专用网络与公用网络的互联环境之中，尤其以接入 Internet 网络为最甚。

15.2.2　防火墙的作用

防火墙的作用通常包括以下几个方面。

1. 防火墙是网络安全的屏障

一个防火墙（作为阻塞点、控制点）能极大地提高内部网络的安全性，并通过过

滤不安全的服务而降低风险。同时，防火墙可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2. 防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。如在网络访问时，一次一密口令系统和其他的身份认证系统完全可以不必分散在各个主机上，而可以集中在防火墙一身上。

3. 对网络存取和访问进行监控审计

如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并做出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。

4. 防止内部信息的外泄

通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。

15.2.3 防火墙的功能

防火墙作为不同安全域间的阻塞点和控制点，极大地提高了内部网络的安全性，它通过过滤不安全的服务而降低风险。从其发生发展的情况来看，防火墙的功能日益成熟。

1. 路由功能

外网口、内网口、DMZ 区不在同一网段时，防火墙启用路由模式，此时的防火墙相当于一台路由器在使用。

2. 地址转换功能

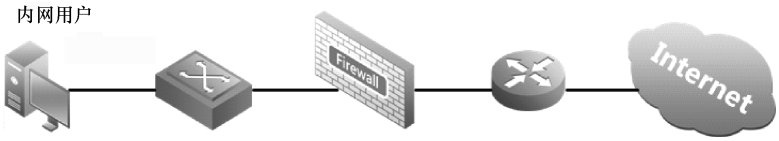
网络地址转换（Network Address Translation，NAT）被广泛应用于各种类型的 Internet 接入方式和网络中。原因很简单，NAT 不仅完美地解决了 lP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

3. 控制访问功能

防火墙以其阻塞点的身份实现监视和控制，通过服务控制、方向控制和用户控制实现访问控制的功能，如图 15-2 所示。

4. 负载均衡功能

负载均衡是一种廉价有效透明的方法，以扩展现有网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性的技术就是负载均衡（Load Balance）。



Access list 100 permit tcp host 192.168.1.3 any eq 80
Access list 100 permit tcp host 192.168.1.3 any eq 21

图 15-2　防火墙控制访问功能示例

5. VPN 功能

虚拟专用网（VPN）被定义为通过一个公用网络（通常是 Internet）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道，保证数据的安全传输。

6. QoS 功能

QoS 的英文全称为“Quality of Service”，中文名为“服务质量”。QoS 是网络的一种安全机制，是在带宽分配、网络阻塞等问题中常用的一种技术。

在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS，比如 WEB 应用，或 E-Mail 设置等。但是对关键应用和多媒体应用就十分必要。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。

15.2.4　防火墙的分类

根据不同的分类方式，防火墙有不同的类别。

从防火墙的存在形式来分的话，可以分为软件防火墙和硬件防火墙。

从防火墙部署的位置来看，可以分为个人防火墙和网络防火墙。本书讨论的是网络防火墙。

从架构实现方式来看，硬件防火墙一般是基于三种平台去实现：X86、NP 架构、ASIC 架构。

从技术原理上讲，防火墙总体来讲可分为四大类：简单包过滤型、状态检测型、应用代理型、内核检测型。

以下将从技术原理角度，对不同类型的防火墙进行更深入地介绍。

1. 简单包过滤型

包过滤型防火墙工作在 OSI 模型的网络层和传输层，它根据数据包包头的源地址、目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则被从数据流中丢弃。

数据包过滤是一个网络安全保护机制，它用来控制流出和流入网络的数据。简单地说，简单包过滤防火墙是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制定。报头信息中包括 IP

源地址、IP 目标地址、传输协议（TCP、UDP、ICMP 等）、TCP/UDP 目标端口、ICMP 消息类型等。

2. 状态检测型

状态检测（Stateful-inspection）防火墙根据其协议及连接状态对穿过防火墙的数据进行检测，可以追踪和控制会话流，支持多种应用，包括 Internet 应用、数据库应用、多媒体应用等。

传统的包过滤防火墙只是通过检测 IP 包头的相关信息来决定数据流的通过还是拒绝，而状态检测技术采用的是一种基于连接的状态检测机制，将属于同一连接的所有包作为一个整体的数据流看待，构成连接状态表，通过规则表与状态表的共同配合，对表中的各个连接状态因素加以识别。这里动态连接状态表中的记录可以是以前的通信信息，也可以是其他相关应用程序的信息，因此，与传统包过滤防火墙的静态过滤规则表相比，它具有更好的灵活性和安全性。先进的状态检测防火墙读取、分析和利用了全面的网络通信信息和状态。

3. 应用代理型

代理防火墙能够比其他类型的防火墙提供更多的安全性，但是，这是以牺牲速度和功能为代价的，因为代理防火墙能够限制你的网络支持什么应用程序。那么，为什么代理防火墙更安全呢？代理防火墙与稳定的防火墙不同，稳定的防火墙允许或者封锁网络数据包进出受保护的网络，而通信流不经过代理。如果使用代理防火墙，计算机要建立一个通向代理的连接，这个代理充当一个中介并且代表这台计算机的请求启动一个新的网络链接。这就阻止了防火墙两端的系统直接进行连接，使攻击者很难发现这个网络在什么地方，因为它们永远不接收它们的目标系统直接创建的数据包。

代理防火墙也对它们支持的协议提供深入的和熟悉协议的安全分析。这使它们能够比那些纯粹以数据包包头信息为重点的产品做出更好的安全决策。例如，一个专门为支持 FTP 协议而编写的代理防火墙能够监视在命令通道上发出的实际的 FTP 命令，并且阻止任何禁止的行为。代理防火墙允许实施熟悉协议的记录。因为服务器是由代理保护的，这种记录能够让人们很容易发现攻击方法并且为现有的记录创建一个备份。

应用代理防火墙是工作在应用层，其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

4. 内核检测型

内核检测技术，即基于 OS 内核的会话检测技术，在 OS 内核实现对应用层访问控制。它相对于包过滤和应用代理防火墙来讲，不但更加成功地实现了对应用层的细粒度控制，同时，更有效保证了防火墙的性能。

内核检测防火墙工作原理如图 15-3 所示。

15.2.5 防火墙应用场景分析

A 股份制商业银行防火墙部署如图 15-1 所示，在不同的功能区域分别部署防火墙

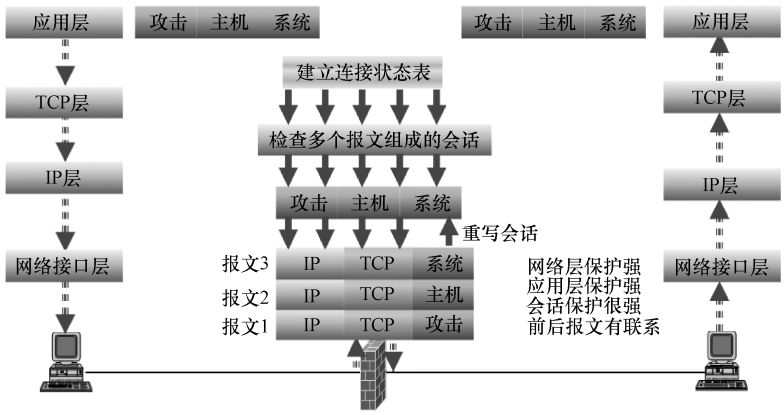


图 15-3　内核检测防火墙

进行单独防护，共有 11 个位置部署了防火墙，分别为 A1 ~ A11。

下面对不同的部署位置进行单独分析：

A1 在移动办公区部署防火墙实现连接互联网接入同时与内网各个区域实现安全隔离。

A2 在开发测试区出口部署防火墙。

A3 ~ A4 在 Internet 网银区域，采用双机部署模式，采用双冗余链路互联，提高业务系统的可用性。

A5 ~ A6 在应用 APP + DB 区域，实现网上银行业务交易处理，提供 APP 与 DB 之间的互访，并于内网前置机进行通信。

A7 ~ A8 在内外网之间采用双机部署模式，实现双冗余链路互联，实现内外网安全隔离。

A9 在第三方支付系统的出口部署防火墙，实现与其他业务系统的隔离和安全防护。

15.3　网络威胁检测与防护技术

15.3.1　IDS 概念

入侵是指在非法或者未经授权的情况下，试图存取或处理系统或网络中的信息，或破坏系统或网络的正常运行，致使系统或网络的可用性、机密性和完整性受到破坏的故意行为。入侵检测，顾名思义，是对入侵行为的发觉。入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术，是通过数据的采集和分析实现对入侵行为检测的技术。

进行入侵检测的软件与硬件的组合便是入侵检测系统（简称 IDS）。入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

15.3.2 入侵检测系统的功能和作用

由于防火墙处于网关的位置，不可能对进出攻击做太多的判断，否则会严重影响网络性能，如果把防火墙比作大门警卫的话，入侵检测系统就是监控摄像机。入侵检测系统通过监听的方式获取网络的运行状态数据，判断其中是否含有攻击的企图，并通过各种手段向管理员报警，不但可以发现外部的攻击，也可以发现内部的恶意行为。

当 IDS 发现一个可疑的恶意威胁（事件）后，它会记录该事件并采取适当的行动。该行动可能是继续登录、发送报警、重定向攻击。如果该威胁是高风险的，IDS 将提醒相关人员。报警可以通过 E-Mail、SNMP、短信发送到移动设备或者控制台。IDS 支持深度安全原理，并可用于检测多种威胁事件。

入侵检测系统的功能很多，比如监测并分析用户和系统的活动；检查系统配置和漏洞；评估系统关键资源和数据文件的完整性；识别已知的攻击行为；统计分析异常行为；对操作系统进行日志管理，并识别违反安全策略的用户活动；针对已发现的攻击行为做出适当的反应，如告警、终止进程等。具体来看，入侵检测系统的功能包括但不限于以下内容：

1）密码破解。
2）协议攻击。
3）缓冲区溢出。
4）模拟尝试。
5）安装工具包。
6）恶意命令。
7）软件漏洞攻击。
8）非法数据操作。
9）未经授权的文件访问。
10）恶意代码，如病毒、木马和蠕虫。
11）拒绝服务攻击。

15.3.3 入侵检测系统的分类

入侵检测系统可以根据多种方式分类，本节介绍两种典型的分类方式，即按照检测原理和数据来源进行分类的方式。

1. 根据检测原理进行分类

(1) 异常检测 异常入侵检测是根据系统或用户的非正常行为或者对于计算机资源的非正常使用而检测出入侵行为的检测技术。在异常检测中，观察到的不是已知的入侵行为，而是系统运行过程中的异常现象。异常检测需要建立一个系统的正常活动状态或者用户正常行为模式的描述模型，操作时将用户当前行为模式或系统的当前状态与该正常模型进行比较，如果当前值超出了预设的阀值，则认为存在着攻击行为。

(2) 误用检测 误用入侵检测系统根据已知入侵攻击的信息（知识、模式等）来检测系统中的入侵和攻击。误用检测需要对现有的各种攻击手段进行分析，建立能够代表该攻击行为的特征集合，操作时将当前数据进行处理后与这些特征集合进行匹配，如果匹配成功则说明有攻击发生。

(3) 混合检测 混合检测指在考虑分析系统正常行为的同时，还观察可以的入侵行为，之后再做出检测结构判断，所以检测结果能更全面、准确和可靠。它通常根据系统的正常数据流背景来检测入侵行为，有人称其为“启发式特征检测”。

2. 根据数据来源进行分类

(1) 基于主机的入侵检测系统（Host-based Intrusion Detection System，HIDS） 基于主机的入侵检测系统通过监测主机的审计记录、系统日志、应用日志及其他辅助数据，来查找和发现攻击行为的痕迹。它可以部署在各种计算机主机上部署。

(2) 基于网络的入侵检测系统（Network-based Intrusion Detection System，NIDS） 基于网络的入侵检测系统使用网络数据包作为数据源，通常实时监视并分析通过网络的所有数据，从中获取有用的信息，再与已知攻击特征相匹配或与正常网络行为原型相比较来识别攻击事件。

(3) 混合式的入侵检测 混合式入侵检测系统将基于主机的入侵检测技术与基于网络的入侵检测技术融合在一块，一方面能够对主机上的用户或进程行为进行监测，另一方面能够对网络的整体态势做出反应。在具体实现上，混合式的入侵检测主要分为两种类型，一种是基于多种监测数据源的入侵检测技术，另一种是采用多种不同类型的检测方法的入侵检测技术。

15.3.4 入侵检测的过程

总的来说，入侵检测的过程可以分为三个阶段：信息收集、信息分析及告警与响应。

1. 信息收集

入侵检测的第一步是信息收集，即从入侵检测系统的信息源中收集信息，包括系统、网络、数据及用户活动的状态和行为等。而且，需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息，这除了尽可能扩大检测范围的因素外，还有一个重要的因素就是从一个源来的信息有可能看不出疑点，但从几个源来的信息的

不一致性却是可疑行为或入侵的最好标识。

2. 信息分析

信息分析是入侵检测过程中的核心环节，没有信息分析功能，入侵检测也就无从谈起。

入侵检测的信息分析方法有很多，如模式匹配、统计分析、完整性分析等。每种方法都有其各自的优缺点，也都有其各自的应用对象和范围。

分析是入侵检测的核心功能，它既能简单到像一个已浏览处理日志的人去建立决策表，也能复杂到一个集成了几百万个处理的非参数系统。

3. 告警与响应

当一个攻击或事件被检测到以后，入侵检测系统就应该根据攻击或事件的类型或性质，做出相应的告警与响应，即通知管理员系统正在遭受不良的入侵，或者采取一定的措施阻止入侵行为的继续。

15.3.5 入侵检测系统的部署与应用

网络入侵检测系统位于有敏感数据需要保护的网络上，通过实时侦听网络数据流，寻找网络违规模式和未授权的网络访问尝试。当发现网络违规行为和未授权的网络访问时，网络监控系统能够根据系统安全策略做出反应，包括实时报警、事件登录，或执行用户自定义的安全策略等。

入侵检测系统可以部署在网络中的核心，监视并记录网络中的所有访问行为和操作，有效防止非法操作和恶意攻击。同时，入侵检测系统还可以形象地重现操作的过程，可帮助安全管理员发现网络安全的隐患。

在图 15-1 中 B1 位置部署 IDS 来保障应用 APP + DB 区域安全，由于 70% 以上的网络攻击事件是发生在传输层和应用层之间，我们称这类 4 ~ 7 层上的攻击为深层攻击行为。传统的防火墙主要在 1 ~ 3 层，对 4 层以上的攻击显得力不从心。为了实现对深层攻击的防御，弥补防火墙等传统安全网关设备的不足，应部署入侵检测系统。入侵检测系统以旁路方式部署，实时分析网络链路上的传输数据，对隐藏在 4 ~ 7 层特别是应用层的攻击行为进行检测。

15.3.6 入侵防御系统与 WEB 应用防火墙

IDS 技术采用了一种预设置式、特征分析式工作原理，所以检测规则的更新总是落后于攻击手段的更新。为了弥补其不足，入侵防御系统（Intrusion Prevention System，IPS）与 WEB 应用防火墙（WAF）应运而生。

1. 入侵防御系统

入侵防御系统（IPS）是一部能够监视网络或网络设备的网络数据传输行为的计算

机网络安全设备，通过串联而非旁路部署，能够实时地中断、调整或隔离一些不正常或是具有伤害性的网络数据传输行为。

对于部署在数据转发路径上的 IPS，可以根据预先设定的安全策略，对流经的每个报文进行深度检测（协议分析跟踪、特征匹配、流量统计分析、事件关联分析等），如果一旦发现隐藏于其中的网络攻击，可以根据该攻击的威胁级别立即采取抵御措施，这些措施包括（按照处理力度）：向管理中心告警、丢弃该报文、切断此次应用会话、切断此次 TCP 连接。

IPS 内部的技术特征包括：

（1）嵌入式运行 只有以嵌入模式运行的 IPS 设备才能够实现实时的安全防护，实时阻拦所有可疑的数据包，并对该数据流的剩余部分进行拦截。

（2）深入分析和控制 IPS 必须具有深入分析能力，以确定哪些恶意流量已经被拦截，根据攻击类型、策略等来确定哪些流量应该被拦截。

（3）入侵特征库 高质量的入侵特征库是 IPS 高效运行的必要条件，IPS 还应该定期升级入侵特征库，并快速应用到所有传感器。

（4）高效处理能力 IPS 必须具有高效处理数据包的能力，对整个网络性能的影响保持在最低水平。

2. WEB 应用防火墙（WAF）

WEB 应用防火墙是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 WEB 应用提供保护的一种技术和产品。

WAF 可以阻止针对 WEB 的各种攻击，譬如：SQL 注入、XSS 攻击、溢出攻击、挂马攻击、盗链攻击、WEB 恶意扫描攻击、CSRF 攻击、XML DoS 攻击、CC 攻击等。

WEB 防火墙产品部署在 WEB 服务器的前面，串行接入，不仅在硬件性能上要求高，而且不能影响 WEB 服务，所以往往不仅具有 HA 功能、Bypass 功能，而且还需要与负载均衡、WEB Cache 等 WEB 服务器前的常见的产品协调部署。

15.3.7 入侵防御系统与 WEB 应用防火墙的部署与应用

在图 15-1 中的 C1 位置部署 IPS 来保障银行网站 WEB 与邮件服务器区域的不受来自 Internet 非正常访问的攻击。

在网银 WEB 服务器区域的 C2、C3 位置部署 IPS 采用双机部署模式，采用双冗余链路互联，提高业务系统的可用性。

A10、A11 的位置部署 WEB 应用防火墙来保障网银系统的安全。

15.4 虚拟专用网络（VPN）技术

VPN 的英文全称是“Virtual Private Network”，翻译过来就是“虚拟专用网络”。顾

名思义，我们可以把它理解成是虚拟出来的企业内部专线。

15.4.1 VPN 基本概念

虚拟专用网络的目的是提供一条安全的网络通道，通常是通过 Internet 的专用隧道。要达到这个目的，需要将传输内容封装在含有目的路由信息的数据包包头信中，这些信息有助于将所传输的内容送达目的地。传输内容通常会进行加密处理，这样能够保证数据的完整性、机密性和可认证性。它可以通过特殊的加密的通信协议在连接到 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通信线路，就好比是架设了一条专线一样，但是它并不需要真正地去铺设光缆之类的物理线路。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。

VPN 通过一个私有的通道来创建一个安全的私有连接，将远程用户、公司分支机构、公司的业务伙伴等跟企业网连接起来，形成一个扩展的公司企业网。

15.4.2 VPN 应用场景

在图 15-1 中，D1、D2 的位置旁路部署 SSL-VPN 时采用旁路双机模式部署，采用双冗余链路互联，可提高业务系统的可用性。

部署第三方支付区域，实现到第三方支付系统间的专线或互联网 VPN 的互通链路，同时也可以安全地接入到网银 WEB 服务器区域、网页 APP 与 DB 服务器区域、网站 WEB 与邮件服务器区域。

15.5 无线局域网安全技术

15.5.1 无线局域网简介

无线局域网络英文全名为 Wireless Local Area Networks，简写为 WLAN。无线网络利用射频（Radio Frequency，RF）技术，使用电磁波，取代传统的双绞铜线所构成的局域网络，在空中进行通信连接，使得无线局域网络能利用简单的存取架构让用户方便联网的效果。

WLAN 具有安装便捷、使用灵活、经济节约、易于扩展等有线网络无法比拟的优点，但是由于无线局域网信道开放的特点，使攻击者能够很容易进行窃听、恶意修改，因此安全性成为阻碍无线局域网发展的最重要因素。

15.5.2 无线局域网面临的威胁

无线网络一般受到的攻击可分为两类：一类是关于网络访问控制、数据机密性保护和数据完整性保护而进行的攻击；另一类是基于无线通信网络设计、部署和维护的独特方式而进行的攻击。对于第一类攻击在，有线网络的环境下也会发生。可见，无线网络的安全性是在传统有线网络的基础上增加了新的安全性威胁。

1）加密算法安全性不足。
2）用户安全意识不强。
3）进行搜索攻击。
4）信息泄露威胁。
5）无线网络身份验证欺骗。
6）网络接管与篡改。
7）拒绝服务攻击。

15.5.3 无线局域网的应用

一般在银行的业务大厅中会通过无线局域网给客户提供上网服务，本书不作详细讲解。

15.6 网络设备安全防护

本节主要讲述如何通过保证网络设备（路由器、交换机等）的安全管理来保证基本的网络安全。

15.6.1 VLAN 划分

虚拟局域网（Virtual Local Area Network，VLAN）是一种建构于局域网交换技术（LAN Switch）的网络管理的技术，网管人员可以借此通过控制交换机有效分派出入局域网的数据包到正确的出入端口，达到对不同实体局域网中的设备进行逻辑分群（Grouping）管理，并降低局域网内大量数据流通时，因无用数据包过多而导致拥塞的问题，以及提升局域网的信息安全保障。

为实现交换机以太网的广播隔离，一种理想的解决方案就是采用虚拟局域网技术。这种对连接到第 2 层交换机端口的网络用户的逻辑分段技术的实现非常灵活，它可以不受用户物理位置限制，根据用户需求进行 VLAN 划分；可在一个交换机上实现，也可跨交换机实现；可以根据网络用户的位置、作用、部门或根据使用的应用程序、上层协议

或者以太网连接端口的硬件地址来进行划分。

使用 VLAN 的优点包括：

（1）控制广播风暴 一个 VLAN 就是一个逻辑广播域，通过对 VLAN 的创建，隔离了广播，缩小了广播范围，可以控制广播风暴的产生。

（2）提高网络整体安全性 通过路由访问列表和 MAC 地址分配等 VLAN 划分原则，可以控制用户访问权限和逻辑网段大小，将不同用户群划分在不同 VLAN，从而提高交换式网络的整体性能和安全性。

（3）网络管理简单、直观 对于交换式以太网，如果对某些用户重新进行网段分配，需要网络管理员对网络系统的物理结构重新进行调整，甚至需要追加网络设备，增大网络管理的工作量。在一个交换网络中，VLAN 提供了网段和机构的弹性组合机制。

从技术角度讲，依据不同原则，VLAN 的划分有以下三种方法：

1）基于端口的 VLAN 划分。

2）基于 MAC 地址的 VLAN 划分。

3）基于路由的 VLAN 划分。

在图 15-1 中，各区域的网络划分均使用到了 VLAN 技术，采用的是基于端口的 VLAN 划分方式，详见图中连接线上的 VLAN 编号。

15.6.2 网络设备的访问控制

网络设备访问控制的主要目的是防止非法用户进入网络设备并对其配置进行非法修改，避免网络瘫痪。

1. 对网络设备访问的控制

（1）通过设置并加密口令实现访问控制 网络设备提供的最基本的安全是在设备访问和配置过程中设置登录口令。如果对设备的访问和配置不加以审查，往往会引发安全问题。例如，有些设备出厂时往往没有设置登录口令或设置一些缺省口令字，而一些管理员就利用这些缺省的口令进行管理，攻击者很容易就找到了一个入口，从而引发安全问题。

（2）对虚拟终端的访问控制 虚拟端口相对于实端口而言，一般根据需要在交换机（或路由器）上虚拟出一些端口，这些端口被称为虚拟终端或虚拟端口。每台 Cisco 设备一般有 5 个缺省虚拟终端，在虚拟终端线路上实施访问控制列表，可以控制谁可以远程登录（Telnet）到该设备。

（3）对 WEB 控制台的访问控制 WEB console 是配置网络设备的另一种常用方法，具有友好的操作界面，使配置网络设备变得更加容易，但同时也引出了一些安全问题。为了使得网络设备的管理与维护更加的便利，许多网络设备厂商都在自己的产品中实现了 HTTP 服务器，以建立一个交叉平台的、易于管理的图形化解决方案。用户可以通过 WEB 图形化界面对网络设备进行管理。多数的网络设备，拥有一整套机制来进行认证和限制 HTTP 远程访问。网络管理员必须牢记，嵌入到网络基础设施设备的 HTTP 客户

机和服务器之间的通讯应当是安全的。

（4）对设备的访问设置不同的权限 网络设备的 super 命令设置的口令用于低级别用户向高级别用户切换时进行验证，类似于 UNIX 系统和 Linux 系统中从普通用户转换到 root 账户时须输入 super 进行切换。网络设备的命令级别共分为 4 级，分别为访问级（0 级）、监控级（1 级）、系统级（2 级）和管理级（3 级），当低级别用户向高级别切换时，输入命令 super［level］，此时如果设置了网络设备的 super 的 password，则只有验证通过后切换才能实现。

（5）控制会话超时及设置警示登录标语消息 如果控制台在特权模式下没有人看管，那么任何用户都可以乘机修改网络设备的配置。而对空闲会话的超时设置可以获得额外的安全保障，默认空闲会话超时时间为 10 分钟，可以通过 exec-timeout 命令改变会话超时时间。

2. 利用 SNMPv3 协议来代替 SNMPv2 协议

简单网络管理协议（Simple Network Management Protocol，SNMP）是一个搜集统计信息并远程监视网络基础设施设备的协议，非常简单。在 V2 版本中，其实根本没有提供任何的安全措施。那时，SNMP 协议都是通过明文传输的，包括密码在内，在网络内的传输都是明文的。所以，是非常不安全的。

为此，建议应该采用 V3 版本，而不要采用 V2 版本。因为 V3 解决了 V2 版本中的一些漏洞。特别值得强调的是，在 V3 版本中，采用了 MD5 算法来验证 SNMP 管理器和代理器之间传递信息。在网络设备中，有 SNMP 两个选项，分别为只读与读写两个模式。

3. SSH 与 Telnet 远程管理协议

在实际工作中，还是习惯通过一些远程管理协议来远程管理网络设备。如果用户需要远程管理的话，则有 SSH 与 Telnet 两种协议可以选择。不过在选择的时候，需要注意一个问题。Telnet 与 SSH 在安全上是相差很大的。

Telnet 是一种远程管理协议，但是，它跟 SNMPv2 版本一样，基本上没有提供可以使用的安全机制，无论是代码，还是用户名与口令，在网络上都是明文传输的。

使用 SSH 来管理网络设备，是因为 SSH 比 Telnet 协议提供了更高的安全性。如其口令与代码在网络中都是通过密文来传输的。

在维护各厂商的网络设备时，其性能、安全性、灵活性是日常管理工作中的三个主要目标。故对于安全性来说，可以借鉴以上的三个建议，为网络设备提供一个安全的管理环境。

15.6.3 网络设备安全配置

为保证能正确地操作路由和交换机，需要进行许多配置工作。这些配置工作包括安装补丁包及对设备进行安全配置来增强安全性。再花费大量时间和步骤来打补丁和加固

网络设备，网络就会更安全。

1. 安装补丁

各个网络设备厂商提供的补丁和更新程序要及时更新。

2. 禁用多余服务

路由器、交换机也像其他通用操作系统（Windows、Linux、Unix 等）一样，也有除了转发数据包之外的服务，可以禁用或保护这些服务来增强网络安全性。

（1）ARP 代理 ARP 带来允许一台主机代表其他真实的主机来响应 ARP 请求，通常在防火墙上使用，用来为受保护的主机代理通信。多数厂商的路由都默认支持 ARP 代理功能，但这会使攻击者实行 ARP 欺骗攻击来对抗不在本地子网或 VLAN 中的主机。

（2）其他服务 所有的路由器都提供许多服务，但如果不需要的话，可以关闭。下面是一些服务样例列表，应该根据实际环境来选择替换。我们需要知道哪些能够在网络环境中使用，哪些是默认开启的，怎么样关闭或防止未授权的人员使用。

1）TFTP 服务。小型文件传输（Trivial File Transfer Protocol，TFTP）服务能够传输路由器系统配置文件或者上传软件更新至路由器。但是 TFTP 并不提供身份认证和授权功能，大多数管理员在需要的时候才会打开此服务。

2）BOOTP 服务。路由器可以通过 BOOTP（Bootstrap Protocol）服务的方式来向客户端提供 DHCP 服务。而在大型企业中通常会有专用的 DHCP 服务器来提供客户端的 IP 地址分配工作，所以需要关闭此服务。

3）网页服务。许多厂商的设备都默认提供了网页服务用于修改配置。如果不需要使用网页的方式管理路由器，应禁止该服务。

4）诊断服务 大多数的路由器都开启了多个基于 UDP 或 TCP 的诊断服务，类似于 Echo、Debug 等。这些调试功能会占用大量资源，并且攻击者也可以通过开启复杂的网络情况下的路由调试功能来占用大量资源，以达到创建 DoS 的目的。如果不是用于故障调试或测试的话，应该关闭这些服务。

15.7 案例介绍：某股份制商业银行网上银行系统网络安全建设实例

网上银行作为银行业利用互联网作为其产品、服务和信息的新型渠道，是其向零售和公司客户提供 7×24 小时、全功能服务的新模式。网上银行提供的服务和产品包括存贷、账户管理、金融顾问、电子账务支付，以及其他一些诸如网络货币等电子支付的产品和服务。作为 21 世纪新兴的在线渠道，改变了传统银行的经营模式，并以其低廉的成本、方便的操作和广阔的前景越来越受到人们的重视。目前，网上银行业务越来越普及，并随着移动互联网和智能终端的快速发展，衍生出了手机银行、短信银行等多种创新服务。从理论上说，网上银行已为客户提供了超越时空的“AAA”式服务，即在任何时候（Any-

time)——为客户提供每年 365 天，每天 24 小时；任何地方（Anywhere)——家里、办公室、旅途中……以任何方式（Anyhow)——电话、互联网、手机、传真、电子邮件、短消息……提供全天候金融服务。

人们在享受网上银行便利性的同时，对网上银行的安全性也感到担忧。不断曝光的网上银行账户被盗事件不禁让人心惊肉跳，连续多年的 3·15 晚会更是把网银安全问题推到了风口浪尖。根据网上银行调查报告结果显示，网上银行安全性仍是广大用户最为担忧的，也是用户最为关心的话题。

随着 A 股份制商业银行互联网业务的迅速开展，A 银行原有的网上银行系统已经不能满足业务发展的要求。同时，为了 A 银行业务系统建设对于网上银行业务的开展需要和 A 银行用户交付的要求，需要升级改造现有的网上银行系统为未来业务开展提供支持，在满足 A 银行网上银行业务安全性的同时，提升其互联网业务的整体安全性。升级改造后的网络将充分考虑当前及未来 3～5 年内 A 银行的业务需求，具有规范化、多业务支撑、安全可靠的专用互联网业务平台，以数据传输为主，同时支持语音和图像的交换与传输，实现数据、语音、视频等多种信息交互业务，同时具备较高的网络安全措施。本案例仅对 A 银行网上银行安全建设中的网络安全部分做了介绍。

1. 项目建设目标

本次项目建设涉及 A 银行数据中心网上银行区域的网络安全系统建设，将充分借鉴银行业先进的设计思想，参考其他金融机构的相关建设经验。建成后的网络安全系统应该完全符合设计标准，满足 A 银行业务的快速发展需求，实现各种渠道的网上交易。满足多线路的交易渠道的流量智能分担和冗余设计多中心站点，满足未来两地三中心或多中心架构，全面提升客户体验和业务连续性。

A 银行目前主要的网上银行业务包括：

（1）个人网上银行业务 为客户提供账户信息查询、转账汇款、投资理财、缴费支付、外汇交易、信用卡服务等一揽子金融业务。

（2）企业网上银行业务 为企业客户提供账户查询、授权审批、银企对账等公司银行服务，以及账户总览、任务中心、预约周期转账、电子工资单、网状授权账户、产业链金融等多种金融服务。

（3）手机银行业务 为移动终端客户量身定制的移动金融服务平台，满足个人、企业、小微客户的金融服务需求，拓展服务渠道，提供丰富的移动金融服务。

2. 项目建设方案

（1）网络安全建设的原则 为满足本项目建设要求，网络安全建设部分将遵循以下原则：

1）强化区域划分原则，对不同的功能区域单独防护。

2）实施边界防御，采取访问控制和检测技术相结合，在实现访问控制基础上，加强安全事件的检测、预警与审计，实时掌握安全威胁，及时分析安全风险，并通过分析结果强化现有的安全配置，保持最佳的安全状态。

3）关键业务系统除加强边界防护外，在关键业务主机上也应采取安全控制措施，并加强变更（系统配置文件及数据）审批、异常流量等安全措施。

（2）网络安全建设的具体内容 本网络安全建设案例将网络访问控制、防拒绝服务攻击、入侵检测与保护、行为审计、恶意代码防范改等多个层面展开。

1）网络访问控制。根据网络安全体系架构设计了以下主要业务区域：

① 互联网接入区域：提供多运营商互联网链路接入，实现智能 DNS 解析等功能。

② 网银 WEB 区域：实现来自互联网用户的 WEB 访问。

③ 应用 APP + DB 区域：实现网上银行业务交易处理，提供 APP 与 DB 之间的互访，并与内网前置机进行通信。

④ 运维管理区域：提供网上银行系统的带外网管和安全系统管理部署。

⑤ 第三方支付接入区域：部署第三方支付系统前置机，实现到第三方支付系统间的专线或互联网 VPN 的互通链路。

以上各个业务区域，通过部署防火墙设备实现各个业务区域的隔离和安全防护，所有关键网络设备均采用双机部署模式，采用双冗余链路互联，提高了业务系统的可用性。

2）网络防拒绝服务攻击。拒绝服务攻击（DoS）的攻击方式有很多种，最基本的也是危害最大的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。由于实施拒绝服务攻击的成本低、破坏力大，也是当前不法分子经常使用的攻击手段之一。

为有效抵御拒绝服务攻击，在每条运营商线路上串接一台防 DDoS 攻击设备，通过控制系统总连接数目、半连接数目、基于协议的连接数控制和基于地址的连接数控制等手段，以防范与抵御最具攻击力的 DoS 攻击。

3）网络入侵检测与保护。由于 70% 以上的网络攻击事件是发生在传输层和应用层之间，我们称这类 4 ~ 7 层上的攻击为深层攻击行为。传统的防火墙主要在 1 ~ 3 层，对 4 层以上的攻击显得力不从心。为了实现对深层攻击的防御，弥补防火墙等传统安全网关设备的不足，应部署入侵检测系统。入侵检测系统以旁路方式部署，实时分析网络链路上的传输数据，对隐藏在 4 ~ 7 层特别是应用层的攻击行为进行检测。

网络入侵检测系统在对数据链路层到应用层的网络数据进行全面分析的基础之上，融合漏洞分析信息，可以对上报的攻击事件进行事先的预分析，达到精确报警的目的。网络入侵检测系统采用基于策略的防护方式，内置了多种默认安全策略集，在上线运行前应根据当前系统现状，选择最适合自己需要的安全策略，以达到最佳防护效果，并可根据预设事件发生的频率来调整使用的安全策略，从而实现减少日志量和自动修改事件风险级别。

4）网络行为审计。网络行为审计是信息安全最重要的方面之一，它是实现安全事件的可追溯性、不可否认性的重要数据来源。网上银行系统由于数据源多、数据量大、数据类型复杂，每日面临大量的非法攻击事件和可疑内部违规事件等，良好的安全审计能力是分析网上银行系统安全状况的必要条件。

网上银行系统行为审计主要包括以下内容：

① 审查内部人员操作安全隐患。由于内部员工违规操作导致的安全问题，根据最新统计资料，对企业造成严重攻击中的 70% 是来自于组织里的内部人员。

② 审查第三方维护人员安全隐患。由于业务需求和人力等诸多原因，银行会将非核心业务外包给设备商或者其他专业代维公司，如何有效地监控设备厂商和代维人员的操作行为，并进行严格的审计，是信息安全的重要工作之一。

③ 审查关键业务系统的访问控制与业务数据流，在减小核心信息资产被破坏或泄漏的同时，有效控制业务运行风险，直观掌握业务系统运行的安全状况。

④ 审查内容包括业务数据流量、用户行为等，应可直观地反映网络环境的安全状况。

5）恶意代码防范。为做好网络边界的恶意代码防范工作，从全网防护的角度出发，在互联网网络边界部署防病毒网关安全设备，对进出网络边界的数据包进行实时检测，有效控制病毒的传播途径。

3. 项目建设成果

上述网络安全建设方案可以很好地满足《网上银行系统信息安全通用规范》的相关安全要求，并符合国家信息安全等级保护对于三级系统的技术措施要求，能够从信息安全工作实际需求出发，有效控制内部安全风险，有助于完善 A 银行信息科技内控与审计体系，满足各种合规性要求。

第 16 章
主机安全

主机是由服务器、终端/工作站等硬件设备与设备内运行的操作系统、数据库及其他系统软件共同构成。主机安全包括了操作系统安全、数据库安全、终端安全等相关内容。本章对主机安全涉及的各方面内容进行了详细叙述。

16.1 主机安全概述

主机安全通过操作系统、数据库管理系统及其他安全软件（包括防病毒、防入侵、木马检测）实现的安全功能来满足。信息系统内的服务器按其功能划分，可分为应用服务器、数据库服务器、网络管理服务器、通信服务器、文件服务器等。终端可分为管理终端、业务终端、办公终端（PC 终端与智能终端）等。

主机是网络上的单个节点，因此主机安全是分散在各个主机系统上的，不像网络安全可以整体考虑，需要针对不同的用途、操作系统及系统软件来分别解决。

主机安全是指通过各种手段，保证主机在数据存储和处理的保密性、完整性、可用性，它包括硬件、固件、系统软件的自身安全，以及一系列附加的安全技术和安全管理措施，从而建立一个完整的主机安全保护环境。

主机安全的要求主要有：身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制。

16.2 主机安全保护要求

2012 年 5 月，中国人民银行关于发布发布了《网上银行系统信息安全通用规范》（JR/T 0068—2012）。虽然该规范是针对网上银行系统，但主机安全部分具有普遍适应性，可作为银行业主机信息安全的通用规范。

1. 基本要求

（1）身份鉴别

1）应对登录操作系统和数据库的用户进行身份标识和鉴别，严禁匿名登录。

2）为不同的操作系统和数据库访问用户分配不同的账号并设置不同的初始密码，禁止账号和密码共享。

3）应要求系统的静态密码在 8 位以上，由字母、数字、符号等混合组成。

4）首次登录系统时应强制修改密码，至少每 90 天更改一次密码，不允许提交与上次相同的新密码。

5）在收到用户重置密码的请求后，应先对用户身份进行核实再进行后续操作。

6）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施：

◇ 通过锁定用户的方式限制连续的访问企图（最多不允许超过 6 次）。

◇ 锁定时间至少设定为 30 分钟或直至管理员为其解锁。

7）应确保对密码进行强效加密保护，不允许明文密码出现。

8）对服务器进行远程管理时，如果数据通过不可信网络传输，应采取加密通信方式，防止认证信息在网络传输过程中被窃听。

9）应采用两种或两种以上的组合鉴别技术对管理用户进行身份鉴别，并且身份鉴别信息至少有一种是不可伪造的，如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息。

10）系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放。

（2）访问控制

1）根据“业务必需”原则授予不同用户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

2）应根据管理用户的角色（例如，系统管理员、安全管理员、安全审计员等）分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

3）应实现操作系统和数据库系统特权用户的权限分离。

4）严格限制默认用户的访问权限，重命名系统默认用户，修改默认用户密码，及时删除多余的、过期的用户及调试用户。

5）严格控制操作系统重要目录及文件的访问权限。

（3）安全审计

1）审计范围应覆盖到服务器和管理终端上的每个操作系统用户和数据库用户。

2）审计内容应包括重要用户行为、系统资源的异常使用和重要信息系统命令的使用、账号的创建分配与变更、审计策略的调整、审计系统功能的关闭与启动等系统内重要的安全相关事件。

3）审计记录包括时间、类型、访问者标识、访问对象标识和事件结果，保存时间

不少于半年。

4）应根据记录数据进行安全分析，生成审计报表，并及时备份到集中的日志服务器上或难以更改的介质上。

5）应保护审计进程，避免受到未预期的中断。

6）应保护审计记录，避免遭受未授权的删除、修改或覆盖：

◇ 只允许具有工作需要的人员查看。

◇ 使用文件完整性监视和变更检测软件保护日志，确保已有的日志被改变时产生报警。

◇ 每天复审所有系统的日志。

（4）入侵防范

1）应能够检测到对重要服务器进行入侵的行为，包括但不限于主机运行监视、特定进程监控、入侵行为监测和完整性检测等，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时进行报警。

2）应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施或在检测到完整性即将受到破坏时进行事前阻断。

3）操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，禁用所有不必要和不安全的服务和协议，移除所有不必要的功能。

4）应及时对主要服务器进行补丁升级。

5）应严格限制下载和使用免费软件或共享软件，确保服务器系统安装的软件来源可靠，且在使用前进行测试。

（5）恶意代码防范

1）应安装国家安全部门认证的正版防恶意代码软件。对于依附于病毒库进行恶意代码查杀的软件，应及时更新防恶意代码软件版本和恶意代码库；对于非依赖于病毒库进行恶意代码防御的软件，如主动防御类软件，应保证软件所采用特征库的有效性与实时性；对于某些不能安装相应软件的系统，可以采取其他安全防护措施来保证系统不被恶意代码攻击。

2）主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

3）应支持防恶意代码工具的统一管理。

4）应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。

（6）资源控制

1）应通过设定终端接入方式、网络地址范围等条件限制终端登录，如部署堡垒机统一管理终端接入。

2）应根据安全策略设置登录终端的操作超时锁定，超时时间应小于 15 分钟。

3）应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况，并提供资源使用异常情况下的报警功能。

4）应设定单个用户对系统资源的最大或最小使用限度。

5）应定期对系统的性能和容量进行规划，能够在系统的服务水平降低到预先规定

的最小值时进行检测和报警。

6）所有的服务器应全部专用化，不使用服务器进行收取邮件、浏览互联网等客户端操作。

2. 增强要求

1）应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。

2）应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

3）应对重要信息资源设置敏感标记。

4）应依据安全策略严格控制用户对有敏感标记的重要信息资源的操作。

16.3 操作系统安全机制

操作系统是安装在计算机等设备上，用来控制其他程序运行，管理系统资源并为用户提供操作界面的系统软件的集合，是连接计算机硬件与上层软件和用户之间的桥梁。操作系统安全是主机安全的基础，主要通过以下机制实现：

1）标识与鉴别：用户身份合法性鉴别、操作系统登录等。

2）访问控制：防止对资源的非法使用、限制访问主体对访问客体的访问权限、DAC&MAC&RBAC。

3）最小特权管理：限制、分割用户及进程对系统资源的访问权限；“必不可少的”权限。

以上机制，归根结底要依靠操作系统的安全配置来实现。

16.3.1 标识与鉴别

标识与鉴别的主要作用是控制外界对于系统的访问。其中标识指的是系统分配、提供的唯一的用户 ID 作为标识，鉴别则是系统要验证用户的身份，一般多使用口令来实现。一旦系统验证了用户身份，就要开始赋予用户唯一标识的用户 ID、组 ID，还要检查用户申请的安全级、计算特权集、审计屏蔽码；赋予用户进程安全级、特权集标识和审计屏蔽码。系统负责检查用户的安全级应在其定义时规定的安全级之内，否则系统拒绝用户的本次登录。

16.3.2 访问控制

1. 访问控制的基本概念

访问控制（Access Control）指系统对用户身份及其所属的预先定义的策略组限制

其使用数据资源能力的手段。通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。

访问控制的主要目的是限制访问主体对客体的访问，从而保障数据资源在合法范围内得以有效使用和管理。

访问控制包括 3 个要素（图 16-1）：

1）主体（Subject，S）：是指提出访问资源的具体请求的实体。

2）客体（Object，O）：是指被访问资源的实体。

3）访问控制策略（Attribution，A）。

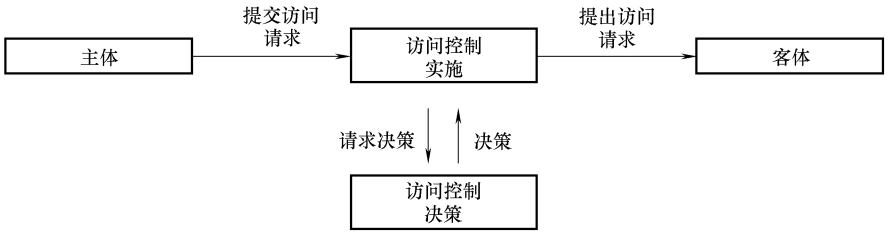


图 16-1　访问控制

2. 访问控制模型

访问控制的主要功能包括：保证合法用户访问授权保护的网络资源，防止非法的主体进入受保护的网络资源，或防止合法用户对受保护的网络资源进行非授权的访问。访问控制的内容包括认证、控制策略实现和安全审计。

访问控制模型是对上述一系列访问控制规则集合的描述，可以是非形式化的，也可以是形式化的。常用的访问控制模型包括自主访问控制、强制访问控制和基于角色的访问控制，如图 16-2 所示。

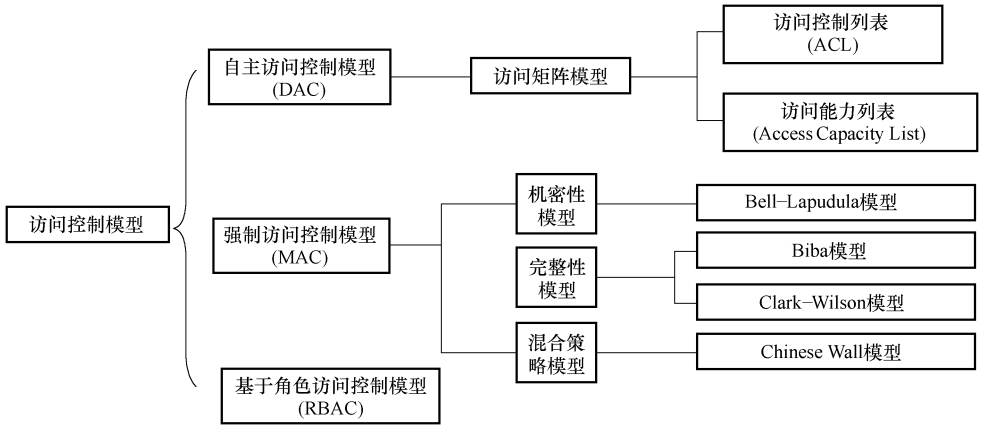


图 16-2　常见的访问控制模型

3. 自主访问控制

“自主”主要体现在客体（访问的对象）的所有者有权指定其他主体对该客体的访问权限，这里的所有者也可以是专门具有授予权限的主体，将权限的子集授予其他

主体。

访问控制矩阵（Access Control Matrix）是实现自主访问控制机制的概念模型，以二维矩阵规定主体和客体间的访问权限。访问控制实现方法包括：访问控制列表（Access Control List，ACL）和访问能力列表（Access Capacity List）。表 16-1 展示了一个基本的访问控制矩阵：主体 S1 对客体 O1、O2、O3 具有 Read 权限，还对 O1 具有 Write 权限；主体 S2 对客体 O2 具有 Write 权限；主体 S3 对客体 O1 具有 Execute 权限，对客体 O3 具有 Read 权限。

表 16-1　访问控制矩阵

主体	客体		
	O1	O2	O3
S1	Read/Write	Read	Read
S2		Write	
S3	Execute		Read

从表中可以看到，任何访问控制策略最终均可被模型化为访问矩阵形式。在访问控制矩阵中行对应于主体，列对应于客体，每个矩阵元素规定了相应的主体对应于相应的客体被准予的访问许可或实施行为。

在具体实现上，访问控制矩阵主要采用以下 2 种方法。

（1）访问控制列表　访问控制列表被定义为一个表，它标识计算机操作系统上的每个用户拥有一个特定的系统对象的访问权限，如文件目录或单个文件的。每个对象都有标识其访问控制列表中的安全属性。该列表具有每个系统用户的访问权限条目。最常见的权限包括读取一个文件或目录中的所有文件的能力、写入到一个或多个文件和执行该文件（如果它是一个可执行文件或程序）的能力，每个操作系统访问控制列表的实现是不同的。比如在 Windows 中，ACL 与每个系统对象息息相关，每个 ACL 具有一个或多个访问控制条目，每个 ACL 包括一个用户或一组用户的名称，用户也可以是一个角色的名字，如程序员或测试人员。对于每个用户、组或角色，访问权限均以比特串表示，称为访问掩码。一般情况下，系统管理员或对象所有者为一个对象创建访问控制列表。

访问控制列表的特点是：访问控制矩阵按列索引，标识出每个客体可以被访问的主体及权限，具体参见图 16-3。

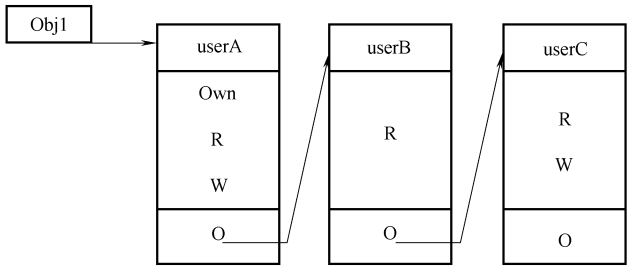


图 16-3　访问控制列表

（2）访问能力列表　访问能力列表是以用户为中心建立的访问权限表。与 ACL 不同，表中规定了该用户可访问的文件名及权限，利用此表可方便地查询一个主体的所有

授权。检索具有授权访问特定客体的所有主体，则需查遍所有主体的访问能力列表。

访问控制列表的特点是：访问控制矩阵按行索引，标识出每个主体可访问的客体及权限，具体参见图 16-4。

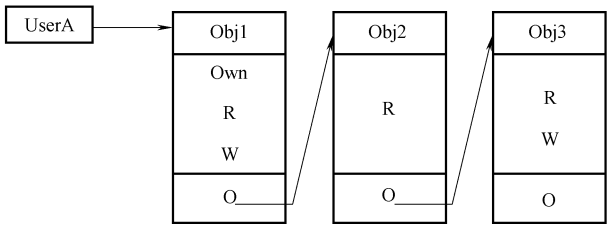


图 16-4　访问能力表

4. 强制访问控制

“强制”体现在每个进程、文件、IPC 客体都被 Administrator 或 OS 赋予了不可改变的安全属性，这些安全属性不能再由用户自己进行修改，实际应用中常常将二者结合起来使用。用户使用自主防止控制防止其他用户非法入侵自己的文件，强制访问控制则作为更有力的安全保护方式，使用户不能通过意外事件和有意识的误操作来逃避安全控制。

强制访问控制（MAC）是系统强制主体服从访问控制策略，是由系统对用户所创建的对象，按照规则控制用户权限及操作对象的访问。主要特征是对所有主体及其所控制的进程、文件、段、设备等客体实施强制访问控制。

MAC 的安全级别常用的为 4 级：绝密级（T）、秘密级（S）、机密级（C）和无级别级（U），其中 T > S > C > U。系统中的主体（用户，进程）和客体（文件，数据）都分配安全标签，以标识安全等级。

基于强制的访问控制，存在不同的安全模型。

（1）机密性安全模型——BLP 模型　BLP 模型是由 D. Elliott Bell 和 Leonard J. LaPadula 于 1973 年提出的一种适用于军事安全策略的计算机操作系统安全模型，它是最早、也是最常用的计算机多级安全模型之一。BLP 将主体定义为能够发起行为的实体，如进程；将客体定义为被动的主体行为承担者，如数据、文件等；将主体对客体的访问分为 r—只读、w—读写、a—只写、e—执行与 c—控制等访问模式，其中 c—控制是用来描述该主体用来授予或者撤销另一主体对某一个客体的访问权限的能力。BLP 的安全策略包括两个部分：自主安全策略和强制安全策略。自主安全策略借助访问矩阵实现，强制安全策略包括简单安全特性和 * 特性，系统对所有的主体和客体都分配一个访问类属性，包括密级和范畴，系统通过比较主体和客体的访问类属性来控制主体对客体的访问。

（2）完整性安全模型——Biba 模型　BLP 模型注重了机密性，但是忽略了完整性保护，于是后人对 BLP 模型进行了一些改进。1977 年 Biba 等人提出了第一个完整性安全模型——Biba 模型，主要应用类似 BLP 模型的规则来保护信息的完整性。Biba 模型提出的不是一个唯一的安全策略，而是一个安全策略系列。比如非自主安全策略里的对

于主体/客体的下限标记策略，使得主体、客体的完整级别动态变化；自主安全策略里的 ACL 和环机制等。

Biba 模型的优势在于其简单性及与 BLP 模型相结合的可能性。简单性体现在 Biba 的严格完整性策略是 BLP 机密性策略的对偶，所以它的实现是直观和易于理解的；基于 Biba 和 BLP 的相似性，二者有可能结合产生集机密性与完整性于一身的安全模型。但是其不足是：

1）完整性标签确定的困难性。

2）Biba 模型最主要的完整性目的是保护数据免受非授权用户的恶意修改，同时其认为内部完整性威胁应该通过程序验证来解决，但是在模型中并没有包括这个要求。

3）Biba 和 BLP 模型的结合看似容易，实则困难，而且即使结合之后，也无法抵御病毒攻击。

（3）完整性安全模型——Clark-Wilson（CW）完整性模型 1987 年 David Clark 和 David wilson 提出的完整性模型具有里程碑意义，它是完整意义上的完整性目标、策略和机制的起源。为了体现用户完整性，CW 模型提出了职责隔离目标；为了保证数据完整性，CW 模型提出了应用相关的完整性验证进程；为了建立过程完整性，CW 模型定义了对于转换过程的应用相关验证；为了约束用户、进程和数据之间的关系，CW 模型使用了三元组结构。

CW 模型的核心在于以良构事务（Well-formal Transaction）为基础实现在商务环境中所需的完整性策略。良构事务是指一个用户不能任意操纵数据，只能用一种能够确保数据完整性的受控方式来操作数据。为了确保数据项仅仅能被良构事务操作，首先得确认一个数据项仅仅能被一组特定的程序来操作，而这些程序是经过验证特殊构造，并且被正确安装的。

（4）多策略安全模型——中国墙（Chinese Wall）模型 1988 年，Brewer 和 Nash 根据现实的商业策略提出了中国墙模型，该模型试图解决的问题是：为了保护相互竞争的客户，咨询公司需要在代理间建立密不可透的“墙”，比如分析员面对客户银行 A、石油公司 A、石油公司 B，一旦分析员访问了石油公司 A（或 B），则都不能再访问石油公司 B（或 A），因为 A 和 B 处于竞争关系，因而用户只能访问其中之一；初始之时用户可以随意访问任意一个客体，但是一旦访问过一个客体，就不能再访问与该客体有竞争关系的其他客体，或者叫不能访问其利益冲突类。这里体现了自由选择和强制控制的微妙组合。

5. 基于角色的访问控制

基于角色的访问控制（RBAC）模型在用户和访问权限之间引入了角色的概念，它的基本特征是根据安全策略划分角色，对每个角色分配操作许可；为用户指派角色，用户通过角色间接地对信息资源进行访问（图 16-5）。

在 RBAC 模型中权限与角色相关联，用户通过取得适当的角色从而获得合适的权限。这可以有效地简化权限管理。在新的应用中同一角色可以授予新的权限，当需要时

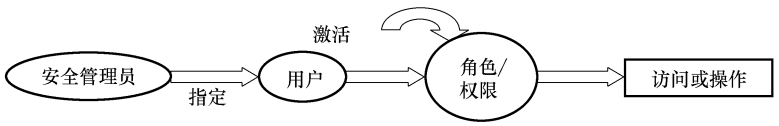


图 16-5　基于角色的访问控制

应用权限可以从角色上被撤销，而无须修改用户的角色，同样可修改用户的角色，使其具有复杂的权限，而不需要修改角色权限。

角色是一定数量的权限的集合，即完成一项任务必须访问的资源及相应操作权限的集合。角色作为一个用户与权限的代理层，表示为权限和用户的关系，所有的授权应该给予角色而不是直接给用户或用户组。

基于角色的访问控制是通过对角色的访问所进行的控制，它使权限与角色相关联，用户通过成为适当角色的成员而得到其角色的权限，可极大地简化权限管理。

RBAC 模型的授权管理方法，主要有 3 种：

◇ 根据任务需要定义具体不同的角色。

◇ 为不同角色分配资源和操作权限。

◇ 给一个用户组（Group，权限分配的单位与载体）指定一个角色。

RBAC 支持 3 个著名的安全原则：最小权限原则、责任分离原则和数据抽象原则。

16.3.3　最小特权原则

最小特权原则是系统安全中最基本的原则之一。所谓最小特权（Least Privilege），指的是在完成某种操作时所赋予系统中每个主体（用户或进程）必不可少的特权。

最小特权原则一方面给予主体“必不可少”的特权，这就保证了所有的主体都能在所赋予的特权之下完成所需要完成的任务或操作；另一方面，它只给予主体“必不可少”的特权，这就限制了每个主体所能进行的操作。

最小特权原则要求每个用户和程序在操作时应当使用尽可能少的特权，而角色允许主体以参与某特定工作所需要的最小特权去签入（Sign）系统。被授权拥有强力角色（Powerful Roles）的主体，不需要动辄运用到其所有的特权，只有在那些特权有实际需求时，主体才去运用它们。如此一来，将可减少由于不注意的错误或是侵入者伪装为合法主体所造成的损坏发生，限制了事故、错误或攻击带来的危害。它还减少了特权程序之间潜在的相互作用，从而使对特权无意的、没必要的或不适当的使用不太可能发生。这种想法还可以引申到程序内部：只有程序中需要那些特权的最小部分才拥有特权。

最小特权在安全操作系统中占据了非常重要的地位，依据“最小特权”原则对系统管理员的特权进行分化，每个用户只能拥有刚够完成工作的最小权限。然后根据系统管理任务设立角色，依据角色划分权限，每个角色各负其责，权限各自分立，一个管理角色不拥有另一个管理角色的特权。如当入侵者取得系统管理员权限后欲访问一个高安

全级别的文件，则很有可能被拒绝。因为用户（包括系统管理员）在登录后默认的安全级别是最低的，他无法访问高级别的文件，而安全级别的调整只有通过安全管理员才能完成。因此，安全管理员只要对敏感文件配置了合理的安全标记，系统管理员就无法访问这些文件。由此可知，最小特权对系统不同角色的权限进行了有力的限制。

16.4 操作系统安全加固

考虑到操作系统结构体系本身的固有缺陷，功能多样性所带来的风险及守护进程与后门存在的可利用漏洞，操作系统安全加固需要针对不同方面的不同特点进行专项配置管理。

1）操作系统结构体系的缺陷。操作系统本身有内存管理、CPU 管理、外设的管理，每个管理都涉及一些模块或程序，如果这些程序里面存在问题，比如内存管理的问题，外部网络的一个连接过来，刚好连接一个有缺陷的模块，可能出现的情况是，计算机系统会因此崩溃。所以，有些黑客往往是针对操作系统的不完善进行攻击，使计算机系统，特别是服务器系统立刻瘫痪。

2）操作系统支持在网络上传送文件、加载或安装程序，包括可执行文件，这些功能也会带来不安全因素。网络的一个很重要的功能就是文件传输功能，比如 FTP，这些安装程序经常会带一些可执行文件，而这些可执行文件都是人为编写的程序，如果某个地方出现漏洞，那么系统可能就会造成崩溃。像远程调用、文件传输，如果生产厂家或个人在上面安装“间谍”程序，那么用户的整个传输过程、使用过程都会被别人监视到，所有的这些传输文件、加载的程序、安装的程序、执行文件，都可能给操作系统带来安全的隐患。所以，建议尽量少使用一些来历不明，或者无法证明它的安全性的软件。

3）操作系统不安全的一个原因在于它可以创建进程，支持进程的远程创建和激活，支持被创建的进程继承创建的权利，这些机制提供了在远端服务器上安装“间谍”软件的条件。若将“间谍”软件以打补丁的方式“打”在一个合法用户上，特别是“打”在一个特权用户上，黑客或“间谍”软件就可以使系统进程与作业的监视程序监测不到它的存在。不过，将传统 root 进行分权可以有效地解决这个问题，如深度操作系统使用 capabi Lities 与审计、系统、安全管理员三权分立的方法可以有效降低特权进程所造成的危害，并将其及早发现。

4）操作系统有些守护进程，它是系统的一些进程，总是在等待某些事件的出现，比如说用户有没有按键盘或鼠标，或者做别的一些处理。一些监控病毒的监控软件也是守护进程，这些进程可能是好的，比如防病毒程序，一有病毒出现就会被捕捉到。但是有些进程是一些病毒，一碰到特定的情况，比如碰到 7 月 1 日，它就会把用户的硬盘格式化，这些进程就是很危险的守护进程，平时它可能不起作用，可是在某些条件发生时，它才发生作用，如果操作系统有些守护进程被人破坏掉就会出现这种不安全的

情况。

5）操作系统会提供一些远程调用功能，所谓远程调用就是一台计算机可以调用远程一个大型服务器里面的一些程序，可以提交程序给远程的服务器执行，如 telnet。远程调用要经过很多的环节，中间的通讯环节可能会出现被人监控等安全问题。解决此问题的方法之一是采用非对称加密通信、最小权限原则与纵深防御。在深度操作系统里缺省，仅在非公知端口开设了 SSL 安全登录，而且通过防火墙限制了有效端口，并限制了远程用户的权限，这样可以有效防御远程调用的攻击。

6）操作系统的后门和漏洞。后门程序是指那些绕过安全控制而获取对程序或系统访问权的程序方法。在软件开发阶段，程序员利用软件的后门程序得以方便修改程序设计中的不足。一旦后门被黑客利用，或在发布软件前没有删除后门程序，容易被黑客当成漏洞进行攻击，造成信息泄密和丢失。此外，操作系统的无口令的入口，也是信息安全的一大隐患。

7）尽管操作系统的漏洞可以通过版本的不断升级来克服，但是系统的某一个安全漏洞就会使得系统的所有安全控制毫无价值。当发现问题到升级这段时间，一个小的漏洞就足以使整个网络瘫痪。

16.5 数据库安全配置

随着信息系统对数据库的依赖性越来越大，拖库现象（数据库中的数据被窃取）频发，盗取数据库的技术在不断提升。虽然数据库的防护能力也在提升，但相比攻击手段来说，单纯的数据库防护还是心有余而力不足。数据库受到的威胁来源如下。

1. 内部人员错误

数据库安全的一个潜在风险就是“非故意的授权用户攻击”和内部人员错误。这种安全事件类型的最常见表现包括：由于不慎而造成意外删除或泄漏，非故意的规避安全策略。在授权用户无意访问敏感数据并错误地修改或删除信息时，就会发生第一种风险。在用户为了备份或“将工作带回家”而做了非授权的备份时，就会发生第二种风险。虽然这并不是一种恶意行为，但很明显，它违反了公司的安全策略，并会造成数据存放到存储设备上，在该设备遭到恶意攻击时，就会导致非故意的安全事件。例如，笔记本电脑就能造成这种风险。

2. 社会工程

由于攻击者使用的高级钓鱼技术，在合法用户不知不觉地将安全机密提供给攻击者时，就会发生大量的严重攻击。在这种情况下，用户会通过一个受到损害的网站或通过一个电子邮件响应将信息提供给看似合法的请求。应当通知员工这种非法的请求，并教育他们不要做出响应。此外，还可以通过适时地检测可疑活动，来减轻成功的钓鱼攻击

的影响。数据库活动监视和审计可以使这种攻击的影响最小化。

3. 内部人员攻击

很多数据库攻击源自内部。当前的经济环境和管理都有可能引起员工的不满，从而导致内部人员攻击的增加。这些内部人员受到贪欲或报复欲的驱使，且不受防火墙及入侵防御系统等的影响，容易给企业带来风险。

4. 错误配置

黑客可以使用数据库的错误配置控制“肉机”访问点，借此绕过认证方法并访问敏感信息。这种配置缺陷成为攻击者借助特权提升发动某些攻击的主要手段。如果没有正确设置数据库的配置，非特权用户就有可能访问未加密的文件，未打补丁的漏洞就有可能导致非授权用户访问敏感数据。

5. 未打补丁的漏洞

如今攻击已经从公开的漏洞利用发展到更精细的方法，并敢于挑战传统的入侵检测机制。漏洞利用的脚本在数据库补丁发布的几小时内就可以被发到网上，当即就可以使用的漏洞利用代码，再加上几十天的补丁周期（在多数企业中如此），实质上几乎把数据库的大门完全打开了。

6. 高级持续性威胁

高级持续性威胁，是指组织（特别是政府）或者小团体利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。其攻击的原理相对于其他攻击形式更为高级和先进，其高级性主要体现在发动攻击之前需要对攻击对象的业务流程和目标系统进行精确的收集，在此收集的过程中，此攻击会主动挖掘被攻击对象受信系统和应用程序的漏洞，在这些漏洞的基础上形成攻击者所需的命令控制网络。其行为没有采取任何可能触发警报或者引起怀疑的行动，因此更接近于融入被攻击者的系统或程序。鉴于数据库攻击涉及成千上万甚至上百万的记录，所以其日益增长和普遍。通过锁定数据库漏洞并密切监视对关键数据存储的访问，数据库的专家们可以及时发现并阻止这些攻击。

16.6 PC 终端安全

对于银行业来说，PC 终端安全分为两大类，一类是内部员工使用的 PC 电脑，它们是内部作业的终端，其安全非常重要；另一类是客户使用网银时所使用的 PC 电脑等设备，它们的安全对网银系统的安全也非常重要，下面分别阐述。

16.6.1 内部 PC 终端安全

内部 PC 终端也是接入内部网络中，其安全对整体的安全十分重要。而目前病毒和木马繁多，传播广泛，对 PC 终端的安全构成巨大威胁，因此有必要采取相关技术来保

证其安全。

（1）终端资产管理 通过对终端的资产注册和管理，确保终端的实名制管理，加强终端网络准入的安全管控和审计，并可以实时监控终端硬件变化，避免硬件或外设的丢失。

（2）终端防病毒管理 通过统一的防病毒平台，对全行的终端实现统一的终端防病毒，以及保障病毒库的实时更新，并实现全行终端病毒感染情况的统计。

（3）终端补丁管理 通过补丁管理，实现终端系统、应用漏洞补丁的验证。多采用统一分发、安装的方式确保补丁的及时修复，减少终端系统的脆弱性，并通过报表展示全行终端的补丁修复率。

（4）终端桌面管理 通过终端桌面管理平台，加强终端的应用安全管理，统一地对终端系统的安全组策略、主机名、外设、安装及运行软件的黑白名单等进行管控，加强终端运行环境的安全性，同时为数据防泄密提供管理手段。

（5）终端准入管理 为确保网络接入终端的合法性和安全性控制，通过统一的终端网络准入管理平台，对所有入网的终端统一采取终端使用人员的身份验证、接入终端资产合法性的验证，接入终端运行环境合法性的验证等手段，来进一步保障全行网络的安全性和稳定性。

16.6.2 客户 PC 终端安全

（1）终端数据安全 近年来，病毒肆虐，电子渠道应确保客户端处理的敏感信息、客户端与服务器交互的重要信息的机密性和完整性；应保证所提供的客户端程序的真实性和完整性，以及敏感程序逻辑的机密性。

（2）终端程序安全 客户端程序应具有抗逆向分析、抗反汇编等安全性防护措施，防范攻击者对客户端程序的调试、分析和篡改。特别需要注意规避各终端平台存在的安全漏洞，例如，按键输入记录、自动拷屏机制、文档显示缓存等。对于移动平台，客户端程序应提供敏感信息机密性、完整性保护功能，如采取随机布放按键位置、防范键盘窃听技术、计算 MAC 校验码等措施。

（3）终端环境安全 银行应采取有效措施提升客户端环境安全级别，例如，在线杀毒服务、安全检测工具等，并在显著位置予以提醒。当发现客户端平台存在重大安全缺陷或安全威胁时，应在门户站点发布警示通知，并通过短信、邮件等方式警示客户。当威胁建模成熟时，可选择使用主动防御，即通过规则判断程序或服务的行为趋势。此种方式可有效降低误报，并从检测方式方面提升客户体验。

16.7 智能终端安全

随着通信技术和移动互联网的高速发展，移动智能终端成为访问互联网的主要方式

之一。由于移动智能终端的功能不断强大和大面积普及，移动智能终端已成为人们日常生活不可或缺的用品。据 IDC 数据显示，2012 年第二季度，中国移动手机出货量达到 8700 万部，其中 51% 为智能手机。在 2012 年全球智能手机市场中，中国市场份额占比达 26.5%，美国占 17.8%，中国已经超越美国成全球最大智能手机市场。

由于移动智能终端本身的开放性、灵活性，以及移动智能终端的广泛应用，给移动用户乃至国家在信息安全方面成极大威胁。移动智能终端面临着各种各样的安全问题，如恶意软件可以控制移动智能终端后台发送短信及后台联网等，造成话费损失；恶意软件还可以在用户不知情的情况下，监听通话、获取用户位置信息、读取和删除用户的个人数据等，造成用户隐私的泄露。

1. 移动智能终端安全架构

移动智能终端安全架构以开放式操作系统为核心，这是移动智能终端的重要特征。移动智能终端的安全架构包括三大层面：硬件层、操作系统层和应用软件层。移动智能终端的安全架构是首先保证安全的硬件，通过安全的硬件绑定安全的操作系统，安全的操作系统绑定安全的应用软件，这样层层绑定从而实现移动智能终端整体的安全。移动智能终端通常有丰富的外围接口，这些外围接口在增强用户体验的同时增加了病毒传播的风险，一些攻击者会通过这些外围接口对移动智能终端进行攻击，从而威胁移动智能终端的安全。另外随着移动智能终端的智能化及存储空间的不断增大，用户的很多重要数据存储在终端中，如通讯录、短信、日程安排等，终端中的大量隐私一旦遭到泄露，那么将对用户造成很大的危害，因此用户数据的保护也是确保移动智能终端安全的非常重要的方面。

2. 移动智能终端面临的威胁

国内移动智能终端服务在迅速发展的同时，原先在 PC 电脑中上演的信息安全问题也在移动终端上再次发生，设备制造商、网络服务商、应用服务提供商和最终客户都已经意识到此问题，并且因为移动智能设备的便利性和时时在线的属性，导致其所面临的信息安全风险更为严重。移动智能终端本身普遍固有的信息安全风险如下：

1）应用与系统软件层：应用软件与数据层包括在操作系统之上运行的各类应用程序、存储和处理的各类数据信息。其主要风险来自于移动恶意软件，可在用户不知情或未授权的情况下自动安装、运行，窃取或篡改终端敏感信息、恶意扣费等，同时也能借助移动网络进行更大范围的恶意传播。

2）操作系统层：操作系统是智能终端上层应用软件运行的基础，提供了丰富、开放的 API 接口，因此会存在功能接口被非法滥用的安全风险，这也是导致恶意软件日益增加的主要原因之一。部分终端操作系统自身隐藏的后门或漏洞使终端存在被远程控制的风险，如 Android 可被 Google 云端服务器远程控制。

3）硬件层：智能终端硬件层主要指其物理器件、芯片及相关驱动等，可能面临探针、电磁辐射监控等物理攻击，这些攻击通过硬件逆向工程或漏洞破解加密算法和密钥等方式窃取或篡改硬件中的敏感数据。较典型的问题如 SIM 卡克隆，目前由于针对硬

件层的攻击成本较高，因此实际发生的案例较少。

3. 移动智能终端安全对应策略

由于移动智能终端的安全威胁可归结为移动智能终端（信宿）、移动应用商店（渠道）和第三方应用服务器（信源）3 个方面，因此应对相关安全威胁的措施手段应主要针对移动智能终端自身安全能力、提供应用软件下载和销售的应用商店及向应用软件提供升级和内容服务的第三方服务器 3 个环节。将这几个关键环节的安全控制住，就能极大地提高移动智能终端的安全。

在移动智能终端环节，通过终端安全技术攻关、安全标准引导及进网管理规范提升终端安全能力。在终端安全技术攻关方面，扶持国内操作系统、芯片等核心技术的研发和产业发展，争取对移动智能终端安全管理的主动权和控制力，加大国家项目中对于移动智能终端的软硬件技术、安全技术、系统软件和应用软件安全漏洞后门分析及处置技术等专项研究的力度，扶持国内企业构建自主可控的移动智能终端安全技术能力与产品方案；在安全标准引导方面，系统梳理并不断完善移动智能终端安全标准体系，推动相关安全标准的制定和贯彻实施，并根据实施情况及时完善标准；在终端进网管理环节，加强对智能终端进网安全检测内容及测试方法手段的研究，补充对硬件芯片及外围接口、用户数据保护、操作系统漏洞、操作系统 API 调用、预置应用等关键环节的安全保障技术和管理措施要求，同时持续跟踪新出现的移动智能终端，如可穿戴设备等，将新型终端及时纳入进网检测。

在移动应用商店环节，积极推进第三方权威认证实验室建设，开展对应用软件、应用商店和第三方服务器的第三方权威安全监测和评估，督促企业落实相关安全要求。此外还需制定针对各类应用软件的安全技术标准，加强对应用软件安全评估工具和方法的研究，保障安全评估高效客观开展。从软件研发源头提高软件质量和安全水平，在软件研发、上线、运行的整个生命周期内实施安全措施保障。对于缺乏应用软件检测能力的移动应用商店经营者，可以要求其委托权威的第三方终端软件测评认证机构按照相关规定代为进行应用软件的测试和认证。

在第三方应用服务器环节，应依照《互联网信息服务管理办法》进一步加强管理。同时，针对境外移动应用商店和新型第三方应用平台的运营者，要与其进行积极沟通，要求其遵守国内的法律法规；远期可通过谈判或法律法规等手段，要求其将服务器搬移到境内，纳入国内法律法规管理体系。同时，要求基础电信运营企业加强业务拨测、内容过滤等安全机制，并要求 IDC/ISP 加强业务接入管理，研究实施 IDC/ISP 层面的恶意代码和不良内容过滤技术手段。

16.8 案例介绍：银行移动智能终端安全

本案例介绍某股份制银行 J 银行为确保移动终端在企业内部的安全所做的工作。

随着消费类电子设备的爆炸式增长，移动终端设备（平板电脑、智能手机等）日

益强大的计算能力和良好的用户体验影响着企业员工的工作习惯和应用体验。2012 年，约有 20% 的企业员工将自己的 iPhone、iPad 或 Android 设备带入工作场所，处理工作等相关事物。然而，手机、平板电脑等移动终端的开放性容易引入各种安全和管理风险。移动终端使得企业办公环境边界进一步延伸，可以在同一台移动设备上处理工作，或在 App Store 上下载喜欢的游戏，企业办公和个人事务瞬息切换，个人和企业应用的界限越来越模糊。对于大多数企业来说，简单地阻止移动终端访问企业应用是不可行的，年轻的员工们出生在一个科技迅速普及的年代，他们对各种移动信息技术并不陌生，迫切希望自己供职的企业能够为他们提供移动终端支持，员工的需求驱使企业必须变更和适应移动终端新技术的变化。同时，开放、智能的移动平台使移动终端成为新的安全缺口，易引入恶意代码植入、个人应用和企业应用混合、数据泄密风险、多平台的异构管理等问题，这些问题给企业信息技术管理带来极大挑战。

（1）不可信终端接入 在传统终端的内外网接入场景下，一般都需要通过安全准入检查，才可接入企业内网。而未实施有效的认证和安全检查的移动终端，若不加控制，则可以绕过限制，直接进入企业内网，使未经授权或染毒的终端接入到企业内网，造成非法用户的访问、攻击或木马的入侵，从而为内网带来安全威胁。

（2）不可信网络传输 在外网移动过程中，尤其是公共场所进行移动办公时，公共 WiFi 热点可能存在 AP 伪造、欺骗、嗅探监听的风险，黑客通过引诱或监视用户上网，进行账号的窃取或者企业机密数据的监听。

（3）不严密的应用管控 在企业业务移动化的冲击下，信息安全制度落后于移动业务的建设速度，应用未经合理合规的安全评估，即向用户开放，可能造成移动用户具有越权访问高机密数据的权限。不合理的访问权限和未实施的审计措施，最终导致泄密事件的发生。

（4）非法的新攻击源 新的移动接入方式可能遭受新的攻击威胁，包括来自移动互联网的攻击和在企业 WLAN 发起的攻击，由于新系统的脆弱性，业务可能遭受严重的干扰。

（5）主动或被动信息泄密 当业务开放给移动终端接入时，业务系统中的敏感数据下载到移动终端本地。而移动终端的位置不确定性及高遗失率和易交换等特点，使得信息扩散尤为便利，从而导致泄密的概率大大增加。

（6）人们期望自己的装备能够随时随地访问公司的数据资源 开放这些访问权限显然有利于提高雇员的工作效率，这与企业利益一致，但同时也会带来安全隐患。每个企业都有一个安全体系，如何扩展这个安全体系的防护功能来确保安全性和合法性，是信息技术安全专家们面临的难题。因此，移动设备管理 MDM（Mobile Device Management）应运而生。目前主流的移动终端操作系统都不同程度地支持移动设备管理协议。今天，新的 MDM 工具集可以根据公司需要来精准管控这些花样翻新的移动设备，控制设备在企业内的功能范围，巩固安全性。据 Nemertes Research 统计，当前有 56% 的公司在使用 MDM 系统，84% 的公司希望在 2014 年年底之前完成 MDM 部署。基于此某股份制银行做了创新式的尝试。

该行经过对以上风险的预测和对多家 MDM 厂商的对比，认为一个完善的 MDM 体

系，是基于生命周期的移动设备管理方案，在功能上为移动设备的获取、部署、运行及回收 4 个生命周期环节提供了完善的 MDM 策略和手段，确保每个环节都能顺畅、安全地实施和开展，又兼顾企业标配机和 BYOD 设备的特点，在确保安全性的同时，不损害用户在使用移动终端时的体验。

1）获取。在移动设备入网初期，应遵循 ITIL 资产管理标准，支持标配机和移动终端的资产发现和注册，并提供移动设备使用承诺协议的自定义模板。

2）部署。在部署 MDM 时要考虑对移动设备上的主机防火墙、VPN 和 WiFi 进行安全配置和策略下发，支持企业安全策略的强制实施。在部署过程中还要考虑对企业移动 App 进行安全的远程分发、安装、配置；企业可以根据用户角色定义 App 黑白名单策略，保证正确的人访问正确的应用和数据。

3）运行。运行阶段重点关注数据和应用的安全性。从密码策略、越狱检测与隔离、外设泄密通道（SIM 卡/SD 存储卡/摄像头/蓝牙/WiFi/USB/录音）的控制，保护在移动终端上使用的数据安全。移动设备容易丢失，MDM 方案应该能够实现对企业关键数据加密，远程锁定/数据擦除。在管理后台，信息技术部门可以审计查询所有移动设备列表，以及相应的状态，如设备型号、操作系统类型与版本等，并可以输出资产审计报表。

4）回收。员工离职或者设备丢失时，为了防止数据泄密，信息技术部门可以对遗留在设备上的应用进行卸载，对数据进行擦除，最后注销此设备。对于企业标配设备，回收的设备可以重新注册绑定，并部署安全策略和应用，移动设备管理生命周期功能示意图如图 16-6 所示。

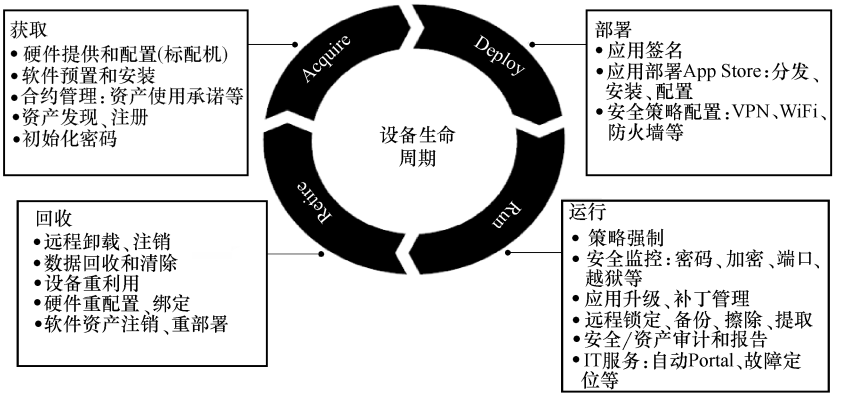


图 16-6　移动设备管理生命周期功能示意图

第 17 章
应用安全

应用安全是继网络、主机系统的安全防护之后，信息系统整体防御的重要防线。但应用系统安全与网络、主机系统安全不同，应用系统一般需要根据业务流程、业务需求由用户定制开发。应用系统安全的实现机制更具有灵活性和复杂性。

应用系统是直接面向最终的用户，为用户提供相关的数据和处理相关信息，因此，它可以提供更多与信息保护相关的功能。

应用安全要求通过应用系统、应用平台系统等实现的安全功能来满足。如果应用系统是多层结构的，一般不同层的应用都需要实现同样强度的身份鉴别，访问控制、安全审计、剩余信息保护及资源控制等，但通信保密性、完整性一般在同一个层面实现。

本章针对应用安全的基本概念、通用要求、基于 WEB 的应用安全等内容进行了详细描述。

17.1 应用安全概述

银行应用安全的总体目标是保障支撑银行业务各类应用的安全，应用安全是业务正常运行的关键。目前，银行业务与外部交互性越来越高，业务越来越复杂，用来支撑业务的应用也越来越多，应用安全是银行业务安全的关键环节之一。

17.2 应用安全通用要求

银行的应用大多关系国计民生，部分操作影响的金额巨大，而用户基数庞大。因此，银行的应用安全，尤其是网银等重要业务，使用环境复杂，其应用安全的要求非常高。应用安全的通用要求包括身份鉴别安全，访问控制安全，安全审计，剩余信息保护，通信完整性、保密性，抗抵赖，软件容错及资源控制。

其中身份鉴别，访问控制，通信完整性、保密性，抗抵赖，对于银行业的关键应用非常重要，它们深度依赖密码技术和密码工具，复杂度很高。同时，银行业务庞杂，需要身份鉴别的应用非常多，例如：电话银行、ATM、POS、网银、3G 互联网等多种电子渠道，还包括大量银行业务衍生的相关金融服务。传统的安全方式基本是各自为战，没有一个统一的客户安全平台。这种方式从安全策略上来讲，无法实施统一的客户安全策略，容易导致安全漏洞。从技术架构来说，没有统一的技术架构，安全技术重复建设。对客户而言，由于没有统一的安全服务平台，客户使用时存在困惑，导致客户体验差。最新的技术都是将客户安全基础设施进行整合，把系统共性的安全要素纳入客户安全平台进行统一管理，并对所有电子渠道提供统一身份鉴别服务的平台，这种平台在银行一般简称安保平台。安保平台是解决银行应用身份鉴别，通信完整性、保密性，抗抵赖等要求的关键技术。

17.3 WEB 应用安全面临的主要威胁

随着信息化进程的不断推进，基于 B/S 模式（即浏览器/服务器模式）的网络信息系统在社会各个领域得到了广泛的应用。银行业务系统也已经从传统的业务模式拓展过渡到新兴的互联网当中，即 WEB 银行系统。据统计，全世界最大的 100 家银行中，20% 已经可以通过 WEB 站点提供在线服务，银行网点数量在一年之内增加了 90%。目前网银业务已经占到传统柜台业务的 30% 以上。据中国银行业协会统计，截至 2014 年金融机构网上银行个人客户已达 2.5 亿户，网上银行企业客户达到 1000 多万户并且发展潜力巨大。

银行业务对 WEB 信息系统的依赖性不断增长的同时，在 WEB 信息系统上运作业务的风险和收益也不断增加，使得 WEB 信息系统的数据库中大量数据的安全问题、敏感数据的防窃取和防篡改问题成为银行信息化管理组织及 WEB 银行系统开发者们越来越关注的内容。

根据国际国内信息安全组织的统计及从银行业信息安全实际来看，WEB 应用安全面临的威胁主要包括以下方面。

1. 注入攻击

注入攻击漏洞，如 SQL，OS 以及 LDAP 注入。这些攻击发生在不可信的数据作为命令或者查询语句的一部分，被发送给解释器的时候。攻击者发送的恶意数据可以欺骗解释器，以执行计划外的命令或者在未被恰当授权时访问数据。

2. 失效的身份认证和会话管理

与身份认证和会话管理相关的应用程序功能往往得不到正确的实现，这就导致了攻击者破坏密码、密匙、会话令牌或攻击其他的漏洞去冒充其他用户的身份。

3. 跨站脚本（XSS）

当应用程序收到含有不可信的数据，在没有进行适当的验证和转义的情况下，就将

它发送给一个网页浏览器，这就会产生跨站脚本攻击（简称 XSS）。XSS 允许攻击者在受害者的浏览器上执行脚本，从而劫持用户会话，危害网站，或者将用户转向至恶意网站。

4. 不安全的直接对象引用

当开发人员暴露一个对内部实现对象的引用时，例如，一个文件、目录或者数据库密匙，就会产生一个不安全的直接对象引用。在没有访问控制检测或其他保护时，攻击者会操控这些引用去访问未授权的数据。

5. 安全配置错误

好的安全需要对应用程序、框架、应用程序服务器、WEB 服务器、数据库服务器和平台定义和执行安全配置。由于许多设置的默认值并不是安全的，因此，必须定义、实施和维护这些设置。这包含了对所有的软件保持及时地更新，包括所有应用程序的库文件。

6. 敏感信息泄漏

许多 WEB 应用程序没有正确保护敏感数据，如信用卡、税务 ID 和身份验证凭据，攻击者可能会窃取或篡改这些弱保护的数据以进行信用卡诈骗、身份窃取，或其他犯罪。敏感数据值需额外的保护，比如在存放或在传输过程中的加密，以及在与浏览器交换时进行特殊的预防措施。

7. 功能级访问控制缺失

大多数 WEB 应用程序的功能在 UI 中可见以前，会先验证功能级别的访问权限。但是，应用程序需要在每个功能被访问时在服务器端执行相同的访问控制检查。如果请求没有被验证，攻击者能够伪造请求以在未经适当授权时具有访问功能。

8. 跨站请求伪造（CSRF）

跨站请求伪造 CSRF，是攻击者利用浏览器自动发送会话 Cookie 等认证凭证，创建恶意的 WEB 页面来产生伪造用户起发的请求，达到攻击目的。CSRF 名称有点类似跨站脚本（XSS），但攻击方式几乎相左。XSS 是利用站点内的信任用户，而 CSRF 则通过伪装来自受信任用户的请求来利用受信任的网站。

9. 使用含有已知漏洞的组件

组件，比如库文件、框架和其他软件模块，几乎总是以全部的权限运行。如果一个带有漏洞的组件被利用，这种攻击可以造成更为严重的数据丢失或服务器接管。应用程序使用带有已知漏洞的组件会破坏应用程序防御系统，并使一系列可能的攻击和影响成为可能。

10. 未验证的重定向和转发

WEB 应用程序经常将用户重定向和转发到其他网页和网站，并且利用不可信的数据去判定目的页面。如果没有得到适当验证，攻击者可以重定向受害用户到钓鱼软件或恶意网站，或者使用转发去访问未授权的页面。

17.4 WEB 安全加固

随着互联网技术的迅猛发展，许多用户的关键业务越来越多地基于 WEB 应用，在通过浏览器方式实现展现与交互的同时，用户的业务系统所受到的威胁也随之而来，并且随着业务系统的复杂化及互联网环境的变化，所受威胁也在飞速增长。

为了应对威胁，WEB 可以通过图 17-1 所示的 4 个阶段进行加固。

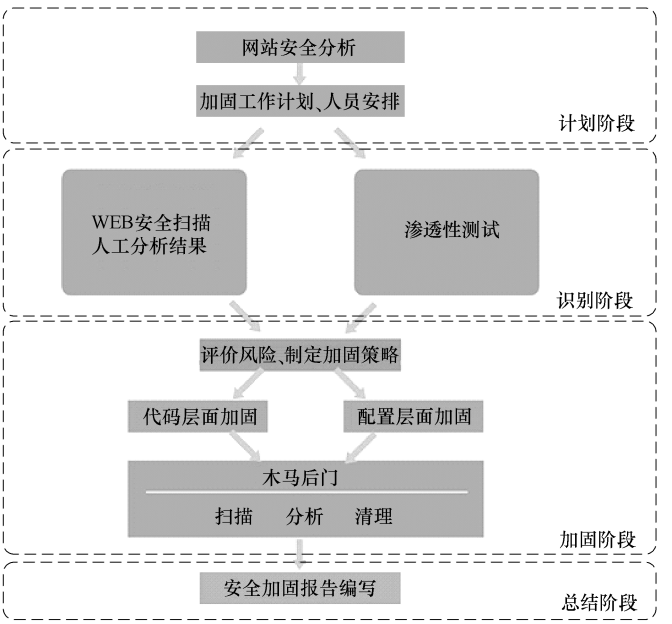


图 17-1 WEB 安全加固流程

这 4 个阶段往往会综合用到以下的 5 个具体方法。

1. WEB 安全扫描

安全检测工作分为 WEB 安全扫描、人工系统分析，在安全扫描中使用专业的 WEB 安全扫描评估工具，通过使用工具进行自动扫描和后期的人工整理分析。

2. 渗透性测试

渗透性测试采用人工配合工具进行检测，通过真实模拟黑客使用的工具、分析方法来进行实际的漏洞发现和利用，最终得到安全检测结果和解决方案。

3. 安全编码

对于跨站、跳转、注入这些漏洞，大多数都是非常简单的不安全编码疏忽所导致的，可以在编码这个阶段通过使用一些安全编码实践来避免。在这个阶段可以提供一些工具的支持，比如静态代码分析，可以分析一些 SQL 注入、跨站脚本，同时可

以提供一些脆弱性测试工具。在这个阶段还要进行重审代码，把残留的不安全代码清理掉。

4. 配置层面加固

根据安全检测的结果，对 WEB 服务器相关配置进行调整，如对 Apache 进行升级，设置合理的目录的权限，关闭不必要的服务方法等。

5. 木马后门处理

对木马文件的常见特征进行研究，并使用木马扫描工具，根据当前的安全规则库，对服务器上的指定目录进行文件的安全扫描，将可疑的文件列出并提供文件查看、删除等操作，避免潜在的安全隐患。

17.5 应用架构安全

应用系统包括很多种类，如 OA、ERP、人力资源管理系统等，本章节以 WEB 应用系统为例来做阐述。

17.5.1 WEB 应用安全的现状及重要性

当今世界，Internet 已经成为一个非常重要的基础平台。很多企业都将应用架设在该平台上，为客户提供更为方便、快捷的服务支持。这些应用的功能和性能，都在不断地完善和提高。然而在安全性上，却没有得到足够的重视。由于网络技术日趋成熟，黑客们也将注意力从以往对网络服务器的攻击逐步转移到了对 WEB 应用的攻击上。然而，绝大多数企业将大量的投资花费在网络和服务器的安全上，没有从真正意义上保证 WEB 应用本身的安全，给黑客以可乘之机，安全风险达到了前所未有的高度。

一个典型的 WEB 应用通常是标准的三层架构模型：第一层是客户端；使用动态 WEB 内容技术的部分属于中间层；数据库是第三层。在企业 WEB 应用的各个层面，都会使用不同的技术来确保安全性。为了保护客户端机器的安全，用户会安装防病毒软件；为了保证用户数据到企业 WEB 服务器的传输安全，通信层通常会使用 SSL（安全套接层）技术加密数据；企业会使用防火墙和 IDS/IPS 来保证仅允许特定的访问。但是，即便有防病毒保护、防火墙和 IDS/IPS，企业仍然不得不允许一部分的通信经过防火墙，而且 WEB 应用是由软件构成的。那么，它一定会包含 bug，这些 bug 就可以被恶意的用户利用，他们通过执行各种恶意的操作，或者偷窃，或者操控，或者破坏 WEB 应用中的重要信息。只要访问可以顺利通过企业的防火墙，WEB 应用就毫无保留地呈现在用户面前。只有加强 WEB 应用自身的安全，才是真正的 WEB 应用安全解决之道。

17.5.2 常见的 WEB 应用漏洞及解决方案

1. WEB 平台软件漏洞

WEB 平台软件漏洞包括 WEB 应用使用的操作系统、HTTP 底层服务器软件（如 IIS 或 Apache）和第三方应用程序中的所有程序错误或者可以被利用的漏洞。这个问题也涉及错误配置，包含有不安全的默认设置或管理员没有进行安全配置的应用程序。其解决方案如下：

1）执行严格的双向网络访问控制。

2）找出系统的安全漏洞，及时更新软件的安全补丁。

3）不要在源代码中放置私密信息。

4）禁用 WEB 服务器上不必要的功能，删除不需要的应用程序。

5）定期扫描入侵者。

2. WEB 认证威胁

WEB 认证包括用户名和口令认证、基于令牌和证书的认证及认证服务。攻击者可以通过用户名枚举、密码猜测和窃听等手段来获取用户名和密码；攻击者还可以通过 SQL 注入绕过认证，也可以窃取用户的 Cookie 并访问用户的账户，而不必输入 ID 和口令或进行其他认证。其解决方案如下：

1）使用强健的密码策略和账户锁定策略。

2）采用高强度的证书，如数字证书。证书认证用户时，同时使用公开密钥系统和数字证书。证书认证还可以和其他基于密码的认证机制一起使用，以提供更强健的安全性。

3）使用 HTTPS 来保护认证传输，避免受到窃听和重放攻击的风险。

4）输入验证可以防止 SQL 注入、脚本注入和命令执行。

5）确保认证安全令牌，如 Session ID 和 Cookie 等，不会被轻易窃取。

3. WEB 授权威胁

授权能够确定经过认证的用户可以访问应用程序的哪些部分，以及他们在应用程序中可执行哪些操作。攻击者通过爬行访问控制列表（ACL）及分析会话（Session）和 Cookie 中保存的信息来得到非法的授权。其解决方案如下：

1）为应用程序定义明确的、一致的访问策略，配置好用户角色。

2）使用 SSL 加密措施防止攻击。

3）不要在会话中包含个人敏感信息。

4）改变权限要重新生成会话 ID。

4. 非法输入和参数篡改漏洞

在数据被输入程序前忽略对数据合法性的检验是一个常见的编程漏洞，它导致 SQL 注入和数据存储攻击、脚本攻击（包括跨站点脚本攻击）和缓冲区溢出等。

注入漏洞，特别是 SQL 注入漏洞，主要是利用目标网站程序未对用户输入的字符进行特殊字符过滤或合法性校验，可直接执行数据库语句，导致网站存在安全风险。

跨站点脚本（XSS）攻击利用网页及 Cookie 漏洞，攻击者往 WEB 页面里插入恶意 jawascript 代码，当用户浏览该页之时，嵌入其中 WEB 里面的 jawascript 代码会被执行，从而达到恶意用户的特殊目的。

参数篡改包括操纵 URL 字符串，以检索用户以其他方式得不到的信息。访问 WEB 应用的后端数据库就是通过常常包含在 URL 中的 SQL 调用来进行的。恶意的用户可以操纵 SQL 代码，以便将来有可能检索一份包含所有用户、口令、信用卡号的清单或者储存在数据库中的任何其他数据。其解决方案如下：

1）对输入数据采用服务器端验证。

2）限制输入字段的长度和数字边界检查以防止缓冲区溢出。

3）对 HTML jawascript 和 SQL 格式中的字符进行编码，如将脚本中的尖括号转化为对应的编码以防止脚本攻击。

4）使用正则表达式查找授权或未经授权的内容。

5）在应用程序中使用参数来构建查询及尽可能地在数据库中使用存储过程。

6）数据库加密。通过表级别和字段级别的加密保护数据。

5. WEB 应用管理漏洞

WEB 应用管理漏洞包括管理员配置错误和开发者错误造成的漏洞，如不必要的 WEB 服务器扩展、直接访问浏览及文件、用户和状态页面信息泄露等。服务器目录浏览是一个不安全的配置，管理员把敏感 log 放在 WEB 目录上，又开放了浏览目录权限，使得黑客直接访问这个目录时，把这些敏感的 log 打开就获取到了明文的用户名、密码。开发人员常常建立一些后门并依靠调试来排除应用程序的故障，这些安全漏洞经常被留存并放在 Internet 上的最终应用中。一些常见的后门用户不用口令就可以登录或者访问允许直接进行应用配置的特殊 URL。其解决方案如下：

1）禁止 IIS 的扩展。

2）保持站点目录整洁并实行正确的访问控制。

3）提高站点开发者的水平和安全意识。

6. WEB 客户端攻击

通过钓鱼软件、间谍软件和恶意广告对在线用户进行欺诈。钓鱼软件通常以精心设计的虚假网页引诱用户上当，达到盗取银行账号、信用卡号码等目的。虚假网页一般以 eBay 和 PayPal 等大家熟悉的网页为招牌，用户点击链接之后就进入了一个看起来与真实网页极其相似的网页。其解决方案如下：

1）运行防病毒软件及反钓鱼和反间谍软件工具。

2）提高警惕，高度谨慎地处理基于 Internet 的请求和事务。

7. 拒绝服务攻击

拒绝服务（DoS）攻击包括计算机网络带宽攻击和连通性攻击。带宽攻击指以极大

的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法通过。连通性攻击指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。其解决方案如下：

1）网络管理员要积极谨慎地维护系统，增强服务器的安全性，确保无安全隐患和漏洞。

2）安装防火墙等安全设备过滤 DoS 攻击。

3）网络管理员应当定期查看安全设备的日志，及时发现对系统的安全威胁行为。

4）在设计 WEB 应用程序时，通过控制用户登录和各种数据处理方式来避免 DoS 攻击。

如尽可能不在客户端做数据处理，尽可能从缓存读取数据库等。

8. 不适当的错误处理

在进行各种错误的处理操作时，应用程序可能由于其不适当的错误处理在无意中泄露其配置信息、内部运作信息及侵犯隐私的敏感信息。攻击者利用该漏洞可能盗取敏感的数据，甚至发动更为危险的攻击行为。其解决方案如下：

1）使用结构化错误处理，以避免使用软件默认的错误处理器而暴露信息。

2）确定结构化错误处理器，即使代码失败，也可以安全地失败。

17.5.3 应用安全开发

软件安全开发的概念始于 20 世纪末 21 世纪初，当时由于病毒猖獗、软件漏洞百出，因软件安全问题导致在现实生活中发生了很多如隐私泄露、资金损失及系统崩溃等安全事件。安全专家由此提出软件安全开发的概念，希望通过在软件开发的各个阶段充分考虑安全因素，来增强软件安全性，并尽量减少软件安全事件的发生。软件的安全性在银行的众多应用系统中显得尤为重要。

软件安全开发的研究主要从生命周期的角度来开展对安全设计的原则、安全开发的方法、最佳实践和安全专家经验等方面的研究，通过采用各种安全活动以保证得到安全的软件。近十年来，众多软件安全开发生命周期被提出来，比较知名的有微软提出的安全开发生命周期（SDL）、使安全成为软件开发必须的部分（BIS）、综合的轻量级应用安全过程（CLASP）、软件保证成熟度模型（SAMM）等。

应用软件安全的目标是要维护信息资源的保密性、完整性和可用性，以确保业务的成功运作。

WEB 应用安全开发的安全编码规范通常包括以下的检查点：输入验证、输出编码、身份验证和密码管理、会话管理、访问控制、加密规范、错误处理和日志、数据保护、通信安全、系统配置、数据库安全、文件管理、内存管理、通用编码规范等内容。

应用开发生命周期通常包括 6 个阶段，分别为需求、设计、开发和测试、部署、运维、废弃阶段，应用安全的问题经常表现在部署、运维阶段，但根源在于需求、设计、开发阶段，安全开发需要将信息安全融入上述阶段中。

17.6 案例分析：应用安全防护案例

某城市商业银行为保障网上银行业务的顺利开展，在网银服务器所在的数据中心分别部署了防火墙、IDS、IPS、链路负载均衡设备等网络安全设备，对于第七层的应用层防护效果不太理想。为了应用层的关键业务的正常运营，在特定的区域（图 17-2 中的 CFCA）部署 WEB 应用防火墙（WAF）、网站监控平台、网页防篡改系统。

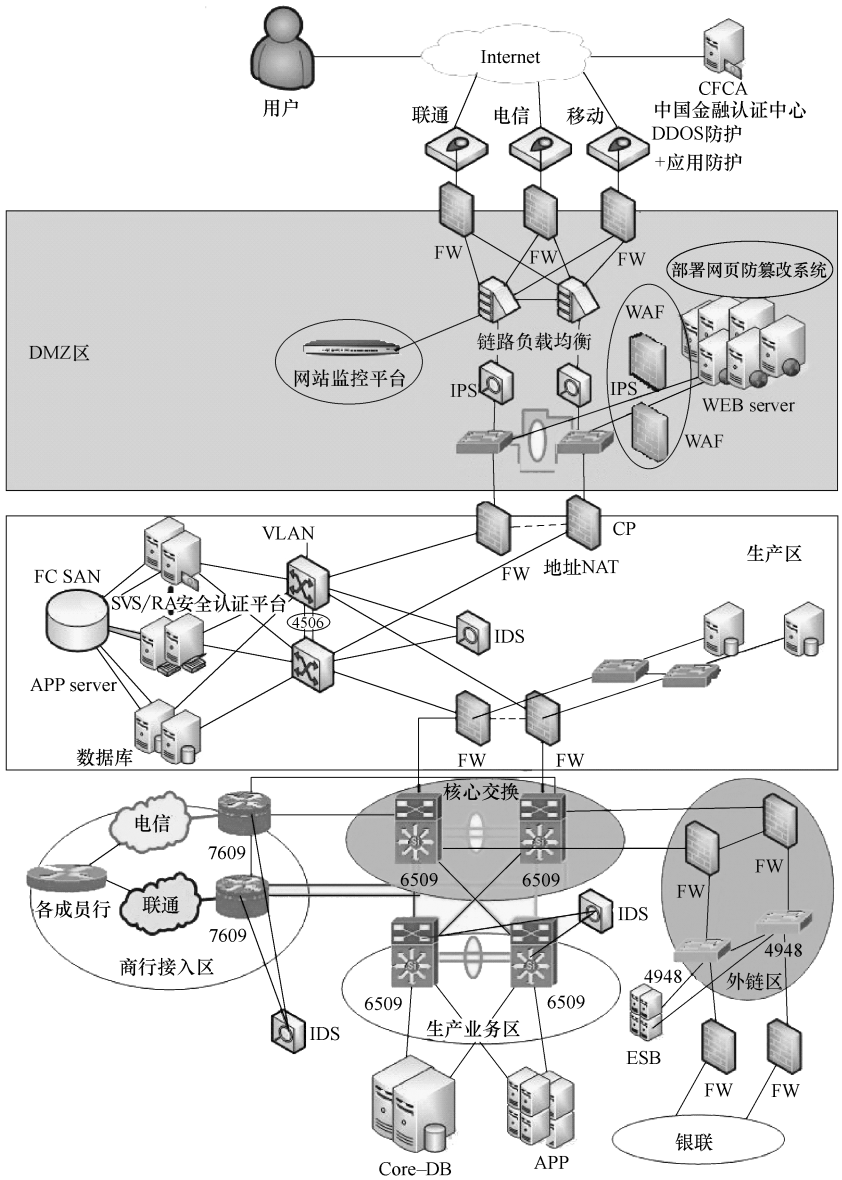


图 17-2　电子银行拓扑图

第 18 章
密码和身份鉴别技术

银行业是国民经济的重要领域，银行信息安全是国家安全的重要组成部分，保障银行业信息安全的方式有很多，密码和身份鉴别技术无疑是非常重要的一种。本章对密码技术的基本概念、身份验证的技术及在银行中的应用进行了介绍。

18.1 密码技术概述

密码技术理论性较强，在全面介绍密码技术的使用前，先对密码技术的基础知识做一个简单的介绍。

密码的发展由来已久，大体分为以下 4 个阶段：

第一个阶段是从古代到 19 世纪末——古典密码（Classical Cryptography）。

第二个阶段从 20 世纪初到 1949 年——近代密码。

第三个阶段从 1949 年 C. E. Shannon（香农）发表的划时代论文“The Communication Theory of Secret Systems”开始——现代密码。

第四个阶段从 1976 年 W. Diffie 和 M. Hellman 发表的论文“New Directions in Cryptography”开始——公钥密码。

1. 古典密码

古典密码是非常古老的密码体系，其大部分加密算法都是使用代替密码或置换密码，有时则是两者的混合。古典密码的使用历史悠久，但现代已经很少使用，在银行业几乎不再使用。

古典密码体制的安全性在于保持算法本身的保密性，受到算法限制，不适合大规模生产，不适合较大的或者人员变动较大的组织。著名的古典密码有恺撒密码和斯巴达人天书密码，分别如图 18-1、图 18-2 所示。

2. 近代密码

近代密码从算法来说与古典密码并没有本质差别，其标志为机械密码/机电密码的

明文字母	abcdefghijklmnopqrstuvwxyz
密文字母	DEFGHIJKLMNOPQRSTUVWXYZABC

图 18-1　恺撒密码

图 18-2　斯巴达人天书密码

产生，用机电代替手工，这可以让其算法变得非常繁复，增加破译的难度，但又不影响加密、解密的速度，在战争中被大量使用。

图 18-3 是著名的转轮密码机 ENIGMA，由 Arthur Scherbius 于 1919 年发明。在二次世界大战期间，ENIGMA 曾是德国陆、海、空三军的最高级密码机。

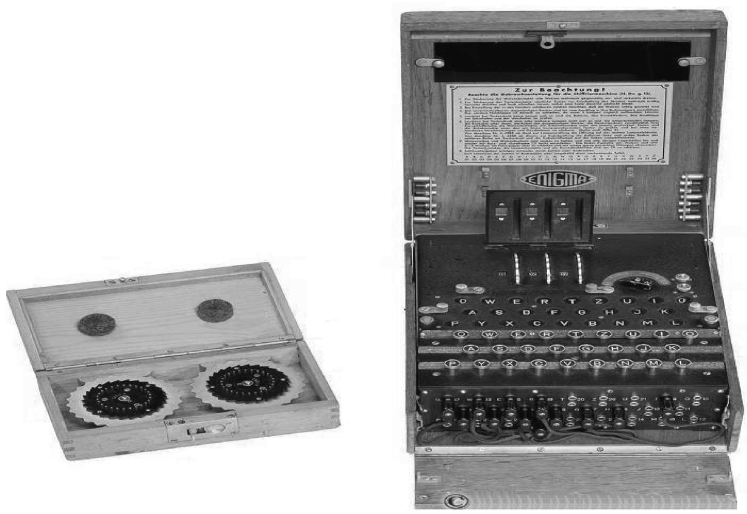


图 18-3　转轮密码机 ENIGMA

近代密码主要用于以前的军事通讯，目前在银行业中也几乎不使用。

3. 现代密码

1949 年，密码学划时代的人物香农（C. E. Shannon）发表划时代论文“The Communication Theory of Secret Systems”，为密码学建立理论基础，从此密码学成为一门科学。Shannon 利用信息论的方法研究加密问题，提出“完善保密”的概念，该文利用数学的方法将信息源、密钥源及密钥做了定量描述和分析，从此以后，主流的数据安全基

于密钥而不是算法的保密，密码技术进入现代密码学。

典型的算法有：DES、3DES、IDEA、AES、国密算法 SM1、SM4、SM7、祖冲之密码等。这些算法一般称之为对称算法，至今在银行业中的使用仍然非常广泛。

4. 公钥密码

1976 年，Diffie 和 Hellman 在发表的论文“New Directions in Cryptography”中提出了非对称密钥密码，即密钥是成对的，分为加密密钥和解密密钥，从一个密钥很难推导出另一个密钥。包含非对称密钥的算法就叫非对称密码算法，又叫公钥密码算法（Public-key Cipher）。其中，对外公开的密钥，称为公开密钥（Public Key），简称公钥；必须保密的密钥，称为私有密钥（Private Key），简称私钥。公钥密码算法的出现使得发送端和接收端之间无须密钥传输，其安全性有显著的提高。

典型的公钥算法有：RSA、ECC、ElGamal、国密算法 SM2、SM9 等。

非对称密码算法除了可以对数据进行加密，还有一个重要的用途是用于实现数据签名。数据签名是只有信息的发送者才能产生的，别人无法伪造的一段数字串，这段数字串同时也是对信息发送者发送信息真实性的一个有效证明。数字签名可以被数据接受者验证，达到抗抵赖的目的，即数据发送者不可以否认自己曾经实际发送过的数据。

5. 散列算法

除加密、解密算法之外，散列算法也是密码算法中非常重要的算法。散列算法又叫哈希（Hash）算法、杂凑算法，是将任意长度的消息映射成一个较短的定长输出信息的算法。其形式为：

$$h = \mathrm{H}(M)$$

式中，M 是变长的报文，h 是定长的散列值。

数学性质：对任意给定的 x，H（x），易于（软硬件实现）计算，且满足：

◇单向性：对任意给定的码 h，寻求 x 使得 H（x）$=h$ 在计算上是不可行的。

◇弱抗碰撞性：任意给定分组 x，寻求不等于 x 的 y，使得 H（y）$=H$（x）在计算上不可行。

◇强抗碰撞性：寻求对任何的（x，y）对，使得 $H(x)=H(y)$ 在计算上不可行。

典型的散列算法很多，常用的如 MD5 和 SHA 系列，以及国密算法 SM3。

18.2 国产密码算法的介绍

银行业是国民经济的重要领域，银行信息安全是国家安全的重要组成部分，国家的相关机构正在从战略层面规划金融领域信息安全的部署和实施。目前中国人民银行在大力推广国产算法的使用，并优先在金融 IC 应用领域展开。密码算法是银行信息安全保障工作的基石，目前我国银行业的密码算法主要采用的仍然是国际的通用算法，如采用 RSA、SHA-1、MD5、DES、3DES、AES 等算法，实现数字签名/验签、数据加密/解

密、密钥协商等安全功能。由于我国无法掌握这些算法设计和应用方面的细节，也就无法从根本上保障金融应用系统的稳定与安全，难以实现自主、可控的信息安全防护体系；同时，随着时间的推移和设备计算能力的提高，某些算法已经不再安全。

为了应对被动局面，国家层面已经进行了统一部署，并研制和公布了 SM2、SM3、SM4 等一系列密码算法，用以保障我国的信息安全。在国家主导的行业中更多地采用国有密码算法，已经成为趋势。为此，中国人民银行也统一推出了国产密码算法应用的总体规划和总体方案，并在实施的时间表上将金融 IC 卡及移动支付等应用排在了最前端。为推动金融 IC 卡与移动支付的发展，中国人民银行启动了《中国金融集成电路（IC）卡规范》的增补和修订工作，于 2013 年发布了 PBOC3.0 规范。与此同时，国家发改委在 2012 年底也专门启动了金融领域 IC 卡和密码应用专项基金，用于扶持和支持相关安全产品，这其中就包括用于 IC 卡的金融数据密码机。事实上，国产密码和算法已经在银行中有相当比例的应用，并在持续地扩大，最终，国产密码和算法将全面取代非国产密码和算法。

国产密码逐步取代非国产密码是金融安全的核心需求，是信息安全技术发展的必然趋势。

2010 年 3 月，美国密歇根大学的三位科学家宣称找到 RSA 算法缺陷，随后国内相关部门也发布了“关于 RSA 算法存在被破解的风险的通报”。为了应对银行业密码算法应用中存在的问题，我国积极推动国产密码算法的研发和使用，国家密码机构制定了一系列密码标准，包括 SSF33、SM1（SCB2）、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法等。其中 SSF33、SM1、SM4、SM7、祖冲之密码是对称算法；SM2、SM9 是非对称算法；SM3 是哈希算法。目前已经公布算法文本的包括祖冲之序列密码算法、SM2 椭圆曲线公钥密码算法、SM3 密码杂凑算法、SM4 分组密码算法等。同时，我国自主知识产权的密码算法及应用条件逐渐成熟，相关部门从国家层面提出实施以国产密码技术为核心的自主可控的金融安全体系建设的战略，并积极开展顶层设计和总体规划。

下面选择银行业最常用的 SM2、SM3、SM4 算法做详细介绍。

18.2.1 SM2 非对称算法

国密非对称算法 SM2 对应国际算法 RSA，其密钥位长为 m（m = 256）。该算法是一种椭圆曲线公钥密码算法，其加解密采用不同的密钥。210 位的 SM2 密钥强度与 2048 位的 RSA 强度相当。关于算法标准，请参见《国家密码管理局公告（第 21 号）》，下面只做简单介绍。

SM2 算法采用的椭圆曲线方程为：

$$y^2 = x^3 + ax + b$$

在 SM2 算法标准中，通过指定 a、b 系数，确定了唯一的标准曲线。同时，为了将曲线映射为加密算法，SM2 标准中还确定了其他参数，供算法程序使用。

本文不探讨椭圆曲线的数学理论，仅通过图示展示算法原理（图 18-4）。

SM2 算法做为公钥算法，可以完成签名、密钥交换及加密应用。SM2 算法标准确定了标准过程：

1）签名、验签计算过程。

2）加密、解密计算过程。

3）密钥协商计算过程。

需要说明的是，其他国家的标准和 SM2 确定的计算过程存在差异，也就是说相互之间是不兼容的。

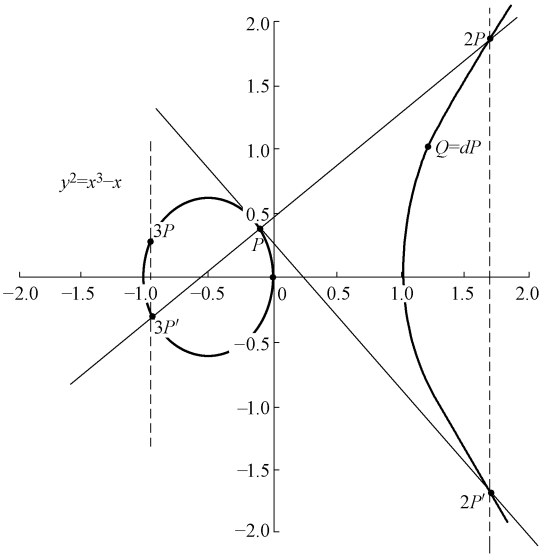


图 18-4　椭圆曲线算法原理

18.2.2　SM3 杂凑算法

杂凑算法 SM3，对应国际算法 SHA-1。对于给定的长度为 k（k < 264）的消息，SM3 密码杂凑算法经过填充、迭代压缩和选裁，生成杂凑值。经预处理过的消息分组长度为 512 位。

SM3 杂凑数据流程如图 18-5 所示。

SM3 杂凑算法流程原理：

1）密码机接收杂凑请求，将数据保存到内存中，并从内存中读取杂凑参数、数据，请求算法卡进行杂凑运算。

2）算法卡接收到数据和杂凑参数后进行杂凑运算，并向密码机 CPU 返回杂凑值。

3）密码机 CPU 接收并向应用返回杂凑值。

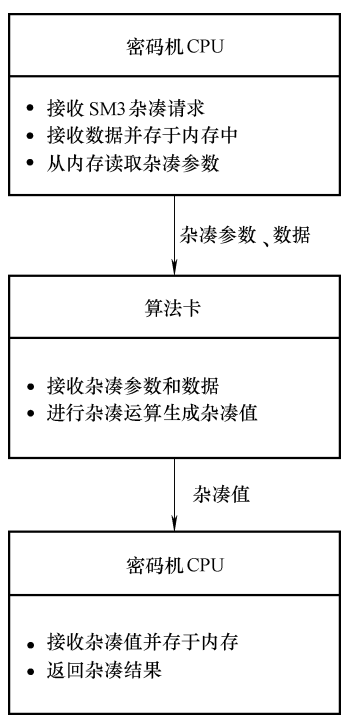


图 18-5　SM3 杂凑数据流程图

18.2.3　SM4 对称算法

国密对称算法 SMS4 对应国际算法 3DES。该算法是一个分组算法，用于无线局域网产品。该算法的分组长度为 128 位，密钥长度为 128 位。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。

此算法采用非线性迭代结构，每次迭代由一个轮函数给出，其中轮函数由一个非线性变换和线性变换复/合而成，非线性变换由 S 盒所给出。

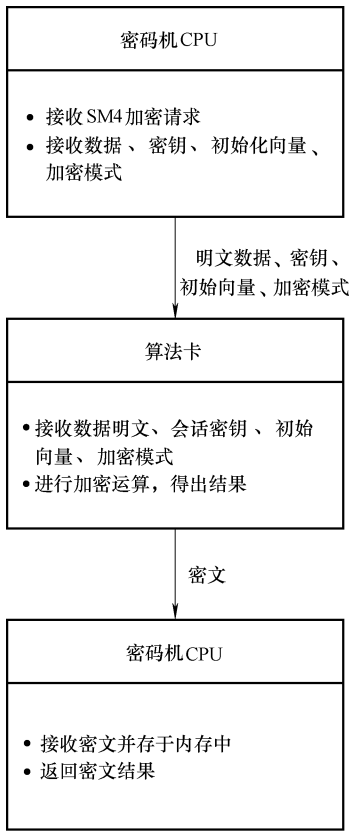


图 18-6　SM4 加密数据流程图

其中 rk_i 为轮密钥，合成置换 T 组成轮函数。轮密钥的产生与 SM3 杂凑数据流程图类似，由加密密钥作为输入生成，轮函数中的线性变换不同，还有些参数的区别。

SM4 加密数据流程如图 18-6 所示。

SM4 加密数据流说明：

1）密码机接收 SM4 加密请求后，将数据、密钥、初始化向量、加密模式保存于密码机内存中，请求算法卡进行加密运算。

2）算法卡接收数据、密钥、初始化向量、加密模式，进行 SM4 加密运算，并将加密结果返回给密码机 CPU。

3）密码机 CPU 接收并向应用返回数据密钥。

18.3　身份鉴别技术

身份鉴别技术是在计算机网络、应用系统中用于确认操作者身份的技术。在信息世界中一切信息包括用户的身份信息都是用特定的数据来表示的，计算机只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。如何保证以数字身份进行

操作的操作者就是这个数字身份的合法拥有者，如何保证操作者的物理身份与数字身份相对应，是作为信息系统入口的第一道关口，有着举足轻重的作用。

银行信息系统，对身份鉴别的要求更高，简单的用户名和密码无法满足银行业务的安全需要。例如，对转账等关键操作，银行业务均要求对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。为实现多种鉴别技术，就需要借助 USBKey、OTP 令牌等安全工具。除这些安全工具外，一些生物识别技术也开始应用，在本部分一并介绍。

18.3.1 业务交易中的身份认证

根据中国人民银行网上银行系统信息安全通用规范对业务安全运作规范中的身份认证做出如下要求：

1）金融机构应按照审慎原则，采取有效、可靠的身份认证手段，保证资金类交易安全。

2）网上银行资金类交易、重要信息及业务变更类等高风险业务应使用双因素身份认证。双因素身份认证由以下两种身份认证方式组成：一是客户知晓、注册的客户名称及密码。二是客户持有、特有并用于实现身份认证的信息，包括但不限于物理介质或电子设备等。以下资金类交易可不受上述限制：同一客户账户之间转账并且金融机构能有效识别转入、转出方为同一客户账户的。

3）禁止仅使用文件证书或使用文件证书加静态密码的方式进行资金类交易。

4）使用企业网上银行进行资金类交易时，应至少使用硬件承载的数字证书进行签名等安全认证方式。

5）应采取有效措施引导客户设置与银行卡交易密码不同的网上银行登录、交易密码，使用不相同的登录密码及交易密码。

6）客户登录网上银行时或登录后执行账户资金操作时，若身份认证连续失败超过一定次数（不超过 10 次），应在短时间内锁定该客户网上银行登录权限或交易账户使用权限，并立即通过短信或电话等可靠的方式通知客户。

7）金融机构用于发送网上银行交易提示短信、动态验证码等信息的客户预留手机号码变更时应符合下列要求之一：客户持有效身份证件到柜台办理；客户通过网上银行渠道变更预留手机号码，金融机构必须采取双因素身份认证验证用户的真实身份及银行卡交易密码，并通过验证发向原预留手机号码的短信验证码等可靠的方式，请求客户本人对预留手机号码变更操作进行确认。

8）网上银行系统接受商户或非金融支付机构的系统建立连接请求时，应通过验证其服务器数字证书、预留 IP 地址比对等方式认证其系统的身份。应对网上银行系统和商户或第三方系统之间发送和接收的信息采用数字证书机制进行签名及验签，保证交易数据的完整性和不可抵赖性。

18.3.2 身份鉴别中常用的安全工具

1. 静态密码

用户密码由用户自己掌握，在系统登录时输入正确的密码，计算机就认为操作者为合法用户。用户的密码是静态存储，平时不会变化，因而叫静态密码。

在实际使用中，由于许多用户为了防止忘记密码，经常采用诸如生日、电话号码等容易被猜测的字符串作为密码，或者把密码抄在纸上放在一个自认为安全的地方，这样很容易造成密码泄漏。同时，验证时，在存储和传输过程中可能会被木马程序或其他手段截获。因此，静态密码机制虽然使用、部署都非常简单，但从安全性上讲，用户名/密码方式一种是不安全的身份认证方式。

静态密码认证还分为本地认证和远程认证，密码保存在本地系统中为本地认证，密码保存在远端的设备中，需要通过网络通信来完成密码认证为远程认证。

银行信息系统对于客户来说，密码均是统一保存在远端的服务器上，均采用远程认证方式。

静态密码最为常见的破解方式为暴力破解，即通过不断尝试密码来寻找正确密码。系统通常设置在登录尝试失败达到一定次数后加以限制，如在一段时间内锁定账号、锁定 IP 等，阻止攻击者连续尝试登录。

2. 智能卡

智能卡（IC Card）是内嵌有微芯片塑料卡的通称。智能卡自身就是功能齐备的计算机，它有自己的内存和微处理器，包括中央处理器 CPU、可编程只读存储器 EEPROM、随机存储器 RAM 和固化在只读存储器 ROM 中的卡内操作系统 COS（Chip Operating System），具备读取和写入能力，允许对智能卡上的数据进行访问和更改，而卡中数据又分为外部读取和内部处理部分。

从安全的角度来看，智能卡提供了对卡片里存储身份认证信息的能力，该信息能够被智能卡读卡器所读取。智能卡读卡器能够连到 PC 上来验证，或者通过 VPN 连接到远程验证。

智能卡由合法用户随身携带，登录时必须将智能卡插入专用的读卡器读取其中的信息，以验证用户的身份。一些智能卡包含一个 RFID 芯片，它们不需要与读写器的任何物理接触就能够识别持卡人。

银行卡就是一种智能卡，类似 ATM 机等业务均利用智能卡结合静态密码验证。

智能卡认证是通过智能卡硬件不被复制来保证用户身份不会被仿冒。然而由于每次从智能卡中读取的数据是静态的，通过内存扫描或网络监听等技术还是有可能截取到用户的身份验证信息，因此还是存在安全隐患。

3. 短信密码/短信验证码

短信密码是以手机短信形式请求包含一些随机数（通常为 6 位）的动态密码，认

证系统以短信形式发送随机的6位密码到客户的手机上，客户在登录或者交易认证时候输入此动态密码，从而确保系统身份认证的安全性。短信密码的优点如下。

1）密码通讯安全性：由于手机与客户绑定比较紧密，短信密码生成与使用场景是物理隔绝的，因此密码在通路上被截取的概率降至最低。

2）普及性：只要能接收短信即可使用，大大降低短信密码技术的使用门槛，学习成本几乎为0，所以在市场接受度上面不会存在阻力。

3）易维护：由于短信网关技术非常成熟，大大降低短信密码系统上马的复杂度和风险，短信密码业务后期客服成本低，是目前银行大量采纳的补充验证技术。

4. 动态口令/动态口令令牌

动态口令（One-Time Password，OTP）又称一次性密码，是使用密码技术实现的在客户端和服务器之间通过共享秘密的一种认证技术，是一种强认证技术，是增强目前静态口令认证的一种非常方便技术手段，是一种重要的补充认证技术，动态口令认证技术由客户端用于生成口令的产生器——动态令牌（一个硬件设备）和用于管理令牌及口令认证的后台动态口令认证系统组成。

动态口令（OTP）的早期意思其实是一次性密码（One-Time Pad，OTP），也叫密电本，是一种应用于军事领域的谍报技术，即对通信信息使用预先约定的一次性密电本进行加密和解密，使用后的密电本部分丢弃不再使用，能够做到一次一密。

目前在安全强认证领域使用的OTP动态密码技术，国内国外均有实用的技术产品支持。比如国内是国密的OTP密码算法，具体使用的是国密SM1（对称）和SM3（HASH）算法。国外最早出现的是RSA公司的RSA SecureID产品，目前，国际上动态口令OTP有两大主流算法，一个是RSA Secure ID，另一个是OATH组织的OTP算法，RSA Secure ID使用AES对称算法，OATH使用HMAC算法。可以说OTP技术已经相当成熟。

动态口令的基本认证原理是认证双方共享密钥，也称种子密钥，并使用同一个种子密钥对某一个事件计数或时间值或异步挑战数进行密码算法计算，使用的算法有对称算法、HASH、HMAC，之后比较计算值是否一致而进行认证。可以做到一次一个动态口令，使用后作废，口令长度通常为6~8个数字，使用方便，与通常的静态口令认证方式类似，使用方便与系统集成好，因此OTP动态口令技术的应用非常普遍，可以应用于多种系统渠道使用，如WEB应用、手机应用、电话应用、ATM自助终端等。动态口令的同步机制有3种，即时间型、事件型和挑战与应答型，目前应用最多的是时间型动态口令，挑战与应答型动态口令的应用也逐渐增多，并且动态口令逐渐变为多种同步类型复合的机制发展，如时间+挑战与应答型。

5. USB Key

基于USB Key的身份认证方式是近几年发展起来的一种方便、安全的身份认证技术。它采用软硬件相结合、一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾。

USB Key 是一种有 USB 接口的硬件设备。它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书，利用 USB Key 内置的公钥算法实现对用户身份的认证。由于用户私钥保存在密码锁中，理论上使用任何方式都无法读取，因此保证了用户认证的安全性。USB Key 产品最早是由加密锁厂商提出来的，原先的 USB 加密锁主要用于防止软件破解和复制，保护软件不被盗版，而 USB Key 的目的不同，它主要用于网络认证，锁内主要保存数字证书和用户私钥。USB Key 也叫 UKEY、USBKey、USB Token，国内习惯翻译成 U 盾，或者优盾。

USB Key 是一种有 USB 接口的小巧硬件设备，形装与常见的 U 盘相似。USB Key 的内部结构复杂，内置 CPU、存储器、芯片操作系统（COS），可以存储用户的密钥或数字证书，可利用 USB Key 内置的密码算法实现对用户身份的认证。每一个 USB Key 都具有硬件 PIN 码保护，PIN 码和硬件构成用户使用 USB Key 的必要因素。用户只有同时取得了 USB Key 和用户 PIN 码，才可以登录系统。即使用户的 PIN 码被泄漏，只要用户持有的 USB Key 不被盗取，合法用户的身份就不会被仿冒；如果用户的 USB Key 遗失，拾到者由于不知道用户 PIN 码，也无法仿冒合法用户的身份。USB Key 具有安全数据存储空间，可以存储数字证书、密钥等秘密数据，对该存储空间的读写操作必须通过程序实现，用户无法直接读取，其中用户密钥是不可导出的，杜绝了复制用户数字证书或身份信息的可能性。USB Key 内置 CPU，可以实现加解密和签名的各种算法，加解密运算在 USB Key 内进行，保证了密钥不会出现在计算机内存中，从而杜绝了用户密钥被黑客截取的可能性。

USB Key 有一代、二代、三代的说法，最早出现的是一代 USB Key（普通型 Key），普通型 USB Key 系列产品是智能密码钥匙产品，无驱无软，即插即用，无须手工操作便自动运行。采用了集成 USB 控制器和 CPU 智能卡的单芯片技术，为产品的先进性和稳定性奠定了良好的基础。普通型 USB Key 系列产品所具有的数据加解密和口令安全存储功能，解决了人们对信息安全管理的需要。普通型 USB Key 系列产品采用标准 USB 接口，外形小巧，便于携带与使用。二代 USB Key（显示型 Key）显示型系列产品是高安全性能智能密码钥匙产品，它在实现普通 USB Key 所有功能的基础上，运用“HIP 人机交互技术”，实现 USB Key 和用户的直接交流，从而有效的防御“远程劫持”和“数据篡改”等黑客攻击手段，确保用户交易的安全性。三代 USB Key（音码 Key）：音码型系列产品是为满足手机银行等应用而产生，在普通型系列产品基础上增加了音码转接头外设，使得音码型系列产品除用于电脑端的网上银行外，也支持手机端的手机银行应用并使得手机银行的终端安全达到二代 Key 水平。一代 Key 主要应用于各个国有银行、商业银行的存量客户，安全性已经不够，在逐步替换更新为二代、三代。

18.3.3 身份鉴别中的生物识别技术

生物识别技术是指通过可测量的身体或行为等生物特征进行身份认证的一种技术。生物特征是指唯一的、可以测量或可自动识别和验证的生理特征或行为方式。使用传感

器或者扫描仪来读取生物的特征信息，将读取的信息和用户在数据库中的特征信息比对，如果一致则通过认证。

生物特征分为身体特征和行为特征两类。身体特征包括声纹（d-ear）、指纹、掌型、视网膜、虹膜、人体气味、脸型、手的血管和 DNA 等；行为特征包括签名、语音、行走步态等。目前部分学者将视网膜识别、虹膜识别和指纹识别等归为高级生物识别技术；将掌型识别、脸型识别、语音识别和签名识别等归为次级生物识别技术；将血管纹理识别、人体气味识别、DNA 识别等归为“深奥的”生物识别技术。

目前使用最多的是指纹识别技术，应用的领域有门禁系统、微型支付等。日常使用的部分手机和笔记本电脑已具有指纹识别功能，在使用这些设备前，无须输入密码，只要将手指在扫描器上轻轻一按就能进入设备的操作界面，非常方便，而且别人很难复制。

下面就在银行系统使用最为广泛的指纹识别技术和最近发展比较快的人脸识别技术做简单介绍。

1. 指纹识别技术

指纹识别即指通过比较不同指纹的细节特征点来进行鉴别。指纹识别技术涉及图像处理、模式识别、计算机视觉、数学形态学、小波分析等众多学科。由于每个人的指纹不同，就是同一人的十指之间，指纹也有明显区别，因此指纹可用于身份鉴定。由于每次捺印的方位不完全一样，着力点不同会带来不同程度的变形，又存在大量模糊指纹，如何正确提取指纹特征和实现正确匹配，是指纹识别技术的关键。

2. 人脸识别技术

人脸识别技术是基于人的脸部特征，对输入的人脸图像或者视频流，首先判断其是否存在人脸，如果存在人脸，则进一步地给出每个脸的位置、大小和各个主要面部器官的位置信息。并依据这些信息，进一步提取每个人脸中所蕴含的身份特征，并将其与已知的人脸进行对比，从而识别每个人脸的身份。

广义的人脸识别实际包括构建人脸识别系统的一系列相关技术，包括人脸图像采集、人脸定位、人脸识别预处理、身份确认及身份查找等；而狭义的人脸识别特指通过人脸进行身份确认或者身份查找的技术或系统。

18.3.4 应用范围

身份认证技术在银行信息系统中的应用极其广泛，对内的工作系统和对外的业务系统均有使用，几乎遍及每个系统。

以对外系统为例，每个账号或者银行卡均有一个基本的密码，这个属于静态密码。在网银等业务中，重要业务安全靠静态密码是无法保证的，一般采用双因素甚至三因素。在双因素中，账号密码或者卡密码是其中一个因素，另外一个因素一般有 USB Key、OTP 动态令牌、短信验证码等。

各安全工具的安全级别、易用性和使用建议如表 18-1 所示。

表 18-1　电子银行渠道安全工具使用建议

安全工具	级别	易用性	能否独立使用（高风险交易）	集成建议
卡交易密码	弱	易	否	建议作为辅助的第二渠道认证方式
手机短信动态密码	弱	易	否	建议作为辅助的第二渠道认证方式
OTP 令牌(时间型)	弱	易	否	强认证工具,建议配合第二渠道认证方式共同使用
OTP 令牌(复合型)	较弱	较易	否	强认证工具,建议配合第二渠道认证方式共同使用
一代 USB Key	较强	较难	否	强认证工具,建议配合第二渠道认证方式共同使用
二代 USB Key	强	难	是	强认证工具,可独立使用

动态口令和 PKI 技术作为主流的强认证方式，在安全特性、客户体验、渠道适用性等方面存在一定的差异。对 OTP 令牌和 USB Key 的安全特性进行比较，见表 8-2，银行应根据自身的业务策略来选择相关技术。

表 18-2　硬件安全设备特性比较

安全工具安全威胁	OTP 令牌(时间型)	OTP 令牌(复合型)	一代 USB Key	二代 USB Key
键盘记录	OK	OK	OK	OK
网络嗅探	OK	OK	OK	OK
强力破解	OK	OK	OK	OK
网络钓鱼	No	OK	OK	OK
中间人攻击	No	OK	No	OK
远程劫持	OK	OK	No	OK
交易篡改	No	OK	OK	OK
交易抵赖	No	No	OK	OK

18.4　案例介绍：密码技术在银行系统的应用实践

互联网、电子商务的发展，促进了金融服务形式的创新，网上银行就是这种创新的具体应用之一。如今人们只需通过一台联网的计算机，便可享受到许多理财服务，如查询、代收费、转账、挂失、咨询、投诉等。然而，网络的开放性与共享性也导致了网络的安全性受到严重影响，如何保证网上数据的安全和交易对方的身份确认是网上银行能否得以推广的关键。可以说，网上银行最关键的问题就是安全问题。密码技术的发展和应用，有助于解决网上银行安全问题，对保证交易信息安全是必不可少的。

1. 密码技术的选用和密钥长度的选择

应用系统研发中若有涉及对数据的加密/解密、签名/验签和完整性保护等安全功能，应从以下密码算法中选用（表 18-3）。

表 18-3　密码算法

密码算法		允许最短密钥长度
算法类型	算法名称	
对称密码算法	3DES/SM4	112 位
非对称密码算法	RSA/SM2	2048 位
散列算法	SHA-1/SM3	不涉及密钥

2. 应用场景

应用系统中所使用的加密技术通常是基于上述各类密码算法的组合，各类主要加密技术使用到的密码算法类型，详见表 18-4。

表 18-4　密码算法对应表

加密技术	使用算法类型	使用算法举例	功能说明
HTTPS/SSL	对称密码算法、非对称密码算法	3DES/SM4、RSA/SM2	建立端到端的安全通道
数字签名	非对称密码算法、散列算法	RSA/SM2、SHA-1/SM3	身份鉴别、防篡改、抗抵赖等
MAC	对称密码算法	3DES/SM4	防篡改

18.4.1　密码技术中的身份鉴别

对于各类身份鉴别信息（如用户身份鉴别信息和服务器之间的身份鉴别信息）的传输和存储过程，应使用密码算法进行加密，以确保安全。

1. 鉴别信息加密传输

1）当使用到普通口令、物理介质、动态口令方式时，若涉及口令的传输，应使用以下安全方式加密传输。

① 使用对称密码算法（3DES/SM4 算法）或散列算法（SHA-1/SM3 算法）加密。

② 采用 HTTPS/SSL 协议。

2）当使用基于 PKI 机制的鉴别方式时，申请验证客户端/服务器应使用私钥对特定信息加密，传输到验证服务器，由验证服务器使用对方公钥解密验证。

2. 鉴别信息加密存储

1）当使用到普通口令、物理介质、动态口令鉴别方式时，若涉及口令的存储，应使用以下安全方式加密存储，且存储加密与传输加密宜采用不同的密钥。

① 使用对称密码算法（3DES/SM4 算法）加密，需要做鉴别信息验证时，直接验证密文。

② 使用散列算法（SHA-1/SM3 算法）加密，需要做鉴别信息验证时，直接验证散列值。

2）当使用基于 PKI 机制的鉴别方式时，宜将私钥保存在智能卡、USB Key 或证书文件中。

3. 数据安全性

1）通信数据机密性保护方式。应用系统内或应用系统间传输的业务敏感数据，可采用以下方式进行机密性保护。

① 使用对称密码算法（3DES/SM4 算法）或散列算法（SHA-1/SM3 算法）加密敏感数据。

② 使用对称密码算法（3DES/SM4 算法）加密传输报文，采用 HTTPS/SSL 协议对所有通信数据加密。

2）不同场景的选用要求。

① 内网传输时，各等级的信息系统应选用以上任意一种方式对敏感数据进行机密性保护。

② 通过互联网对外（如第三方合作单位或个人/企业客户）提供服务时，重要应用系统应选用后两种方式之一对传输的所有数据进行机密性保护；次重要应用系统应选用任意一种方式对传输的敏感数据进行机密性保护。

③ 通过专线网络对外（如第三方合作单位或个人/企业客户）提供服务时，应选用以上任意一种方式对传输的敏感数据进行机密性保护。

18.4.2 密码通信数据完整性保护的应用

1. 通信数据完整性保护方式

应用系统内或应用系统间传输的业务敏感数据，除了采用通信协议和普通校验码（未采用加密技术计算的校验码）等方式，还应对关键系统采用以下加密技术进行完整性保护。

1）散列值。选取通信包中的全部（或关键）数据字段用散列算法（SHA1）计算散列值，随其他通信数据发送给接收方，由接收方重新计算并核对，以检查其完整性是否遭到破坏。

2）安全校验码（MAC）。选取通信包中的全部（或关键）数据字段，使用对称密码算法（3DES/SM4）计算安全校验码（MAC），并随其他通信数据发送给接收方，由接收方重新计算并核对，以检查其完整性是否遭到破坏。

3）数字签名。选取通信包中的全部（或关键）数据字段，使用散列算法（SHA1）和非对称密码算法（RSA/SM2）计算数字签名，并随其他通信数据发送给接收方，由接收方重新计算并核对，以检查其完整性是否遭到破坏。

2. 不同场景的选用要求

内网传输时，对于主机应用系统和重要开放平台应用系统间的通信可选择任意一种方式对敏感数据做完整性保护。

1）通过互联网对外（如第三方合作单位或个人/企业客户）提供服务时，次重要级开放平台应用系统应采用安全校验码（MAC）或数字签名方式对敏感数据做完整性

保护，且应支持密钥/证书的更换；重要级开放平台应用系统应采用数字签名方式对传输的敏感数据做完整性保护，且应支持密钥/证书的更换。

2）通过专线网络对外（如第三方合作单位或个人/企业客户）提供服务时，重要级开放平台应用系统应采用安全校验码（MAC）或数字签名方式对敏感数据做完整性保护，且应支持密钥/证书的更换。

3. 存储数据的机密性保护

对于主机应用系统和重要级开放平台应用系统的敏感数据，应使用对称密码算法（3DES/SM4）加密存放。

4. 剩余信息保护

数据加密/解密、签名/验签等程序中，用于暂时存放密钥的内存，使用前应做初始化处理，在使用完应将其空间内容全部清除。

18.4.3 银行国密算法改造实例

1. 背景

互联网安全日益重要，随着密码技术和计算技术发展，国内密码领域所广泛采用的1024 位 RSA 密码正在面临严峻的安全挑战；基于椭圆曲线的密码算法作为高安全性、高效率的公钥密码，具备和 RSA 算法同样的加/解密、电子签名和密钥协商等重要的密码功能，但与 RSA 相比，它拥有更强的安全性、更高的运算性能等优点。

为了提升商业密码的安全性，大力推广国密算法 SM2、SM3、SM4 的应用和落实，中办机要局起草了《2013 年金融信息系统国产密码算法应用实施工作安排》，要求商业银行在 2013 年年底前，在基础软硬件产品符合应用需求的前提下，完成对网银相关应用软件进行适应性改造和验证。某股份制银行 A 行响应国家要求，实施国密算法改造。

2. 改造内容

1）改造数字证书系统。

① 升级 XX 银行网上银行 PKI 证书发放管理系统，使其全面支持国密 SM2、SM3、SM4 算法；

② 升级民 XX 行网上银行数字证书应用程序，在电子签名、证书验签、数字信封、密钥协商及双向证书认证支持基于 SM2 算法的证书及协议；

2）改造动态令牌系统。

① 改造离线密钥系统，完成银行主密钥和厂商密钥生成和导出功能改造，使其支持国密 SM4 算法。

② 改造管理平台，完成动态令牌密钥种子生成和密钥种子转密算法改造算法，使其支持国密 SM4 算法。

③ 增加动态口令生成算法，使其支持国密 SM4 算法。

3. 数字证书改造方案

1）SSL 安全通讯。SSL 安全通讯采用 SM2 证书，采用 SSL 单向认证（应用中间件、网络设备、浏览器均需支持 SM2 证书）。

2）身份认证。客户端认证：客户端数字证书采用 CFCA 国密 SM2 数字证书。

3）USB Key。采用支持国密算法的 USB Key。

4）签名、验证。采用支持国密算法的签名控件对信息进行签名，并且采用支持国密算法的验签服务器对信息进行验签。

5）加密、解密。采用支持国密算法的工具包组件对信息进行加密、解密。

数字证书改造的网络拓扑图如图 18-7 所示。

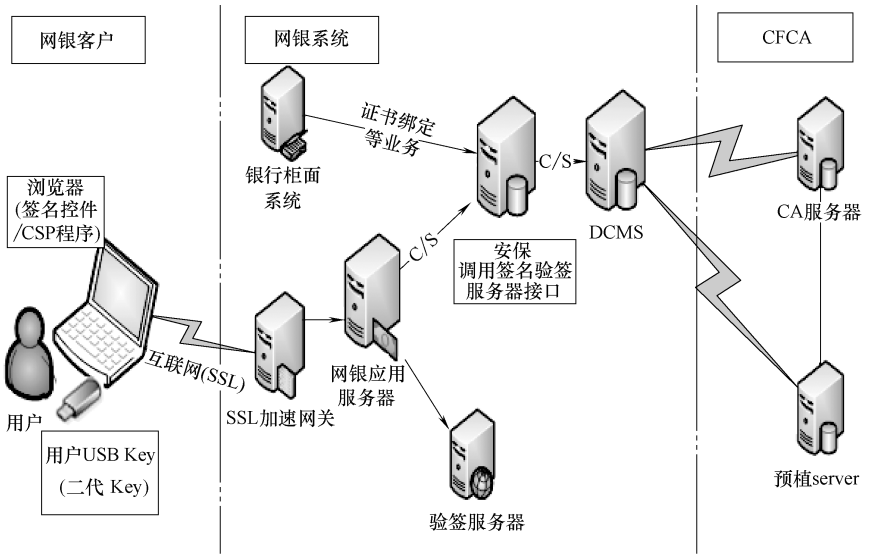


图 18-7　数字证书改造的网络拓扑图

4. OTP 令牌改造方案（图 18-8）

1）离线密钥系统升级。

① 将银行主密钥生成算法改为国密算法 SM4。

② 将厂商密钥生成算法改为国密算法 SM4。

③ 动态令牌软令牌国密算法 SM4 实现。

2）客户安全平台管理平台系统升级。

① 导入主密钥功能，增加导入 SM4 算法生成的主密钥功能。

② 导入厂商密钥功能，增加导入 SM4 算法生成的厂商密钥功能。

③ 令牌密钥种子生成算法改为 SM4 算法。

④ 令牌种子转密算法改为 SM4 算法。

⑤ 管理平台动态令牌测试管理。

3）客户安全平台认证系统升级。增加生成动态口令算法（SM4）。

4）令牌厂商转密系统升级。厂商密钥种子解密算法升级。

5）集成调试。此次改造涉及离线密钥系统、客户安全平台管理平台、客户安全平台认证平台、动态令牌生产厂商、动态令牌设备测试。

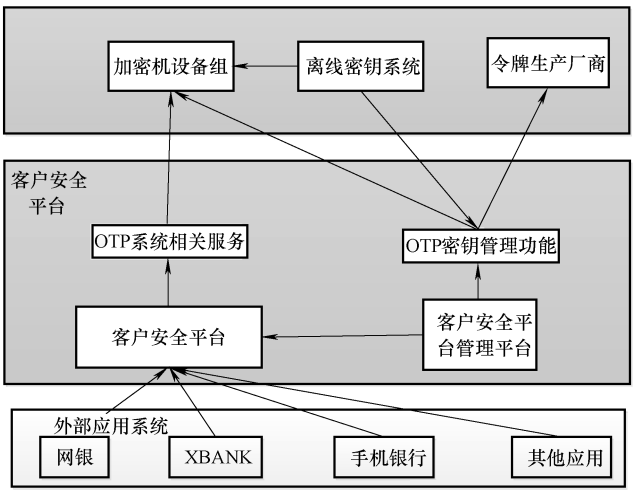


图 18-8　OTP 金牌改造方案

5. 总结

通过对数字证书和令牌口令的改造，A 行成功实现了国产加密算法的支持，为国家金融的安全做出应有的贡献。

密码技术在银行体系中的应用范围非常广，是信息安全的重要基石；国密算法的使用对国家金融安全非常关键，使用范围会越来越广泛。从业人员必须了解密码的原理和应用特点，根据实际业务需求，选择合适的密码技术来保证业务的安全。

18.4.4　加密机在银行中的应用

随着银行业务电子化和网络化的发展，加密机早已经深入应用于各银行业务的数据安全体系中。

1. 加密机的功能

加密机的主要功能有以下两种。

1）支持对 PIN 的所有操作。如产生 PIN、打印 PIN、转换 PIN、加密 PIN 及转换 PIN 的保护密钥、校验 PIN、产生 MAC、验证 MAC、验证并转换 MAC、MASTER 卡 CVC（卡有效码）、VISA 卡 CVV（卡校验值）、PIN 偏移量 Offset 处理机制等。

2）支持非对称算法。如产生非对称算法的密钥对、能够使用公钥加密、使用私钥解密、使用密钥进行数字签名、使用密钥进行签名验证、将密文数据在两个公钥间进行密文转换等。

2. 加密机在发卡系统中的作用

发卡系统包含主机（或服务器）、打卡机、加密机和密码信封打印机。图 18-9 显示了这些设备在发卡系统中的关系。

发卡过程分为预发卡和打卡两个阶段。在预发卡阶段，主机产生将要发的每张 IC 卡的私有信息（如密钥的产生、数字签名、初始密码等），这些私密信息全部由主机调用加密机产生并进行加密处理。在打卡阶段，发卡系统完成卡片的私有化工作，包括将私有信息写入卡片及其他卡片的制作工作。在有需要的情况下，可以提供密码打印，密码信封的打印是使用连接在加密机上的密码信封打印机完成，以保证用户密码的安全。

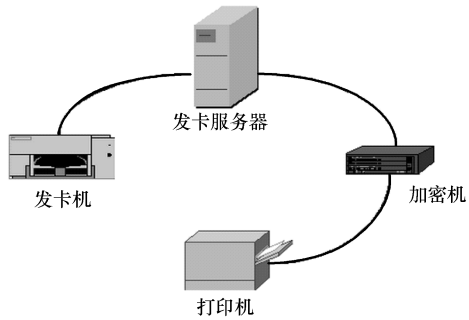


图 18-9　发卡系统中各设备的关系

3. 加密机在交易系统中的应用

在联机交易中，加密机保证交易数据的私密性（关键信息加密）和完整性（MAC 计算和校验），并在发卡行主机端完成相应的认证功能。

通常终端发起的连接交易需要经过前置机及相关中转机构（收单行及银联等金融网络机构）到达发卡行业务系统。在每一个交易节点均需要加密机来保证交易的完整行、保密性等功能，如图 18-10 所示。

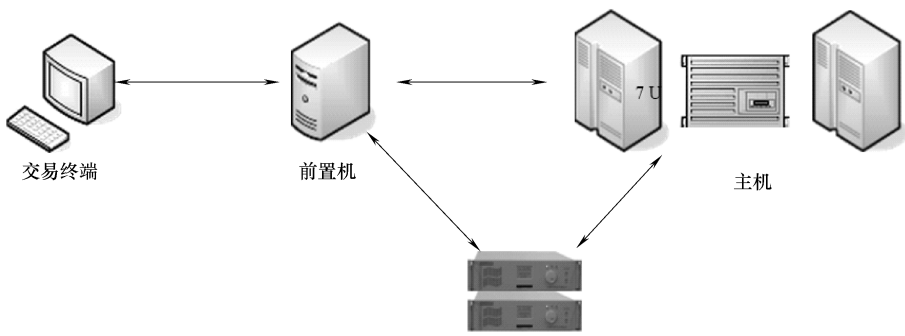


图 18-10　加密机的工作流程

18.4.5　密钥管理平台

当前，金融业大规模采用密码技术为关键信息资产提供保密性、完整性和可用性的保护，大多使用密钥集中管理平台，为银行各业务系统提供密钥全生命周期的安全管理。

密钥集中管理平台主要是针对银行提供的一套对称密钥体系的集中密钥管理系统，提供密钥的生成、分发、更新、存储、注销和使用的全生命周期管理，实现了密钥、密

钥使用策略和密码设备的集中管理，为不同的业务系统提供统一和高性能的密钥服务。

密钥集中管理平台从逻辑上分为三层：平台接口层、平台服务层和平台设备层，如图 18-11 所示。平台接口层主要为业务系统提供各种统一的开发接口；平台服务层是整个系统的核心层，负责在平台接口层和平台设备层之间搭建一个信息处理通道；平台设备层集中管理平台所调用的所有密码设备，并且动态调用密码设备进行密钥的管理操作。

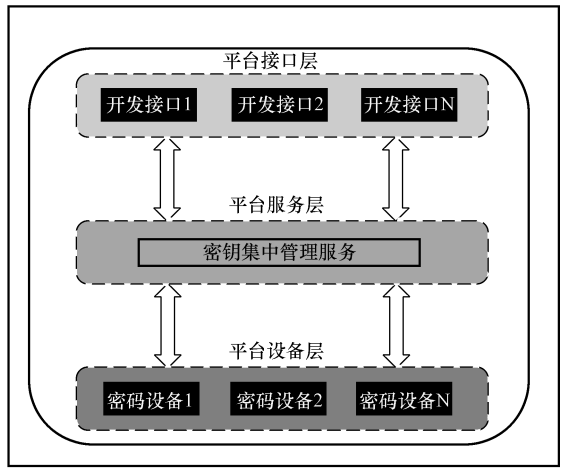


图 18-11　密钥集中管理平台的逻辑结构

密钥集中管理平台采用三级密钥体系对密钥进行管理（图 18-12），包括本地主密钥（LMK）、传输主密钥（ZMK、TMK 等）和工作密钥（ZPK、ZAK、TPK、TAK 等）。其中本地主密钥用于加密密钥，传输主密钥和工作密钥用作本地存储；传输主密钥也成为密钥加密密钥（KEK），用于加密在网络中需要传递的工作密钥，从而实现数据密钥的自动分配，不同的两个通讯网点使用不同的密钥加密密钥，从而实现密钥的分工管理；工作密钥用于应用系统与终端（机构）之间的 PIN 转换、MAC 校验、报文加解密等。

密钥集中管理平台对外提供的接口功能主要包括：传输主密钥的生成和更新、工作

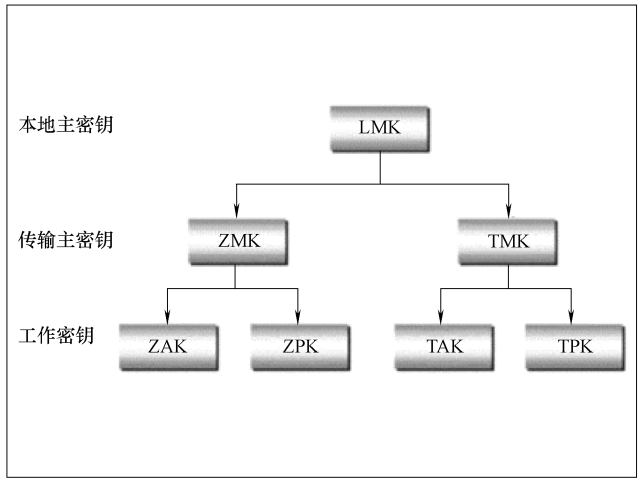


图 18-12　密钥集中管理平台的三级密钥体系管理

密钥的生成和更新、密钥的重置和注销、PIN 转换、MAC 生成和校验等。

密钥集中管理平台具有以下特点：

1）实现密钥的生成、分发、更新、存储、注销和使用的全生命周期的管理。

2）提供简单易用的密钥服务接口。

3）实现密钥及密钥使用策略的集中管理和密钥的安全存储。

4）实现了密码设备的集中管理。

密钥集中管理平台不但实现了密钥及密钥使用策略的集中管理，还实现了对密码设备的集中管理，主要包括密码设备的动态添加和删除；对密码设备的调用进行负载均衡；密码设备运行状态及压力情况的实时监控。当前的密钥集中管理平台在支持国际通用密码算法的基础上，全面支持国家密码管理局公布的 SM3 和 SM4 等国产密码算法，为银行信息安全建设提供必不可少的安全支持。

18.5 案例介绍：身份鉴别技术在银行系统中的应用实践

18.5.1 身份鉴别技术在网银中的应用

某商业银行推出网银系统，该系统的身份认证主要有两个地方：登录和支付。登录部分主要使用静态密码 + USB Key 认证，支付部分则采用双因子认证：用卡密码 + USB Key/OTP 令牌/短信密码。

（1）网银登录场景 在网银登录页面提示客户安装密码安全控件和签名控件。客户插入 USB Key 后，系统根据证书 DN 信息查询签约的网银登录用户名，客户输入登录密码和图形验证码进行登录。客户也可以直接输入登录名或签约卡号直接登录。

客户输入的登录密码使用密码控件和公钥进行加密，加密原文中包含随机数等信息保证客户端输入信息安全。

（2）网银转账场景 客户在转账页面输入转账金额、收款人账号和户名，提交后，网银根据客户的操作系统、浏览器、转账金额大小、转出账号开户号、是否同名转账和客户已签约的安全工具（USB Key/OTP 令牌/短信密码），列出客户可选择的安全工具列表，由客户进行选择，客户提交申请并使用相应的安全工具进行身份认证和交易签名。

18.5.2 身份鉴别技术在手机银行系统中的使用

某商业银行鉴于智能手机的发展推出手机银行，该手机银行是专为移动终端客户量身定制的移动金融服务平台，包含丰富的移动金融服务。

手机银行系统受限于手机系统自身能力和插口，不能使用与网银相同的身份认证方式，该行经过研究，制定针对性的业务流程，并采用以卡密码和短信密码为主的身份认证方式，主要应用于自动签约手机银行、登录、转账。

（1）自助签约手机银行

1）手机银行根据客户输入的卡账户和密码进行卡密码验证，如果是信用卡签约，先调用信用卡前置对密码密文进行转密；如果不是信用卡，调用客户安全平台进行校验，返回校验结果。手机银行获取卡密码校验结果，如果校验失败，提示错误信息；校验通过后进行客户手机号确认。

2）手机银行调用客户安全平台向签约手机号发送短信激活码。

3）客户输入短信激活码，调用客户安全平台的短信验证服务，并返回短信验证结果。

4）手机银行获取短信验证结果，如果验证失败，会提示错误信息；若验证通过，则调用客户安全平台的设置密码服务，并返回设置结果给手机银行。

5）手机银行接收到密码设置结果，显示给客户。

（2）手机银行登录

1）客户在手机银行系统中输入登录的账户和密码。

2）调用客户安全平台的验证登录密码服务，对客户输入的密码进行验证，并返回验证结果。

3）手机银行获取密码验证结果，如果验证失败，会提示错误信息；若验证通过，则返回成功信息。

（3）客户转账

1）客户在进行转账、付款、汇款、存款、取款、话费充值、基金购买、基金定投等操作时需要对卡 PIN 进行验证。

2）客户输入卡号，输入卡 PIN。

3）手机银行调用客户安全平台的卡 PIN 验证服务，对客户输入的卡 PIN 进行验证，只有验证通过才能进行下一步操作。

第 19 章
数据安全

数据安全与备份恢复有着紧密的联系，由于银行信息的重要性，对于备份恢复有着非常高的要求，并有相应的法规文件单独要求，本书将灾难恢复与备份部分作为独立一章阐述。

19.1 数据安全概述

数据安全通常有两方面的含义：一是数据本身的安全，主要是指采用现代密码算法对数据进行主动保护，如数据保密、数据完整性、身份双向认证等；二是数据防护的安全，主要采用现代信息存储手段对数据进行主动防护，如通过磁盘阵列、数据备份、异地容灾等手段保证数据的安全。

早期银行的金融产品相对较少，主要是以存贷汇为主，且数据是以省（市）为单位分布存放，数据量相对较少；此外由于还没有数据集中分析挖掘的需求，日常处理对象主要是短期之内的数据，时间跨度小，处理的数据规模相对可控。

随着各家银行实施了数据大集中，集中存放和处理的数据量急剧增加，随着各类业务的快速发展，银行每天都在产生大量的数据，并需要对这些数据进行分析挖掘，系统资源开销和运行效率都面临着越来越大的压力。例如：某大银行核心数据已达 300T，数据仓库存放的数据已达 400T，全部数据的体量更是难以估量。

为控制在线数据规模、保证应用系统健康高效运行，对数据从创建到最终销毁的生命周期进行全程管理和安全显得越来越迫切。

数据安全是一种主动的防护措施，必须依靠可靠、完整的安全技术体系与安全管理体系来实现。数据安全的内容可以概括为下列的 3 个基本点。

1. 保密性

保密性又称机密性，是指个人或团体的信息不为其他不应该获得者获取到。在现有的信息系统中，大多数软件包括邮件软件、浏览器等，都有保密性相关的设定，用来维

护信息的保密性。在现实环境中，数据的保密性面临多种威胁，如间谍软件、黑客等，都是保密性的威胁源。

2. 完整性

数据完整性是指在传输、存储信息或数据的过程中，确保信息或数据不被未授权的篡改或在篡改后能够被迅速地发现。在实际的信息系统中，完整性常常和保密性边界混淆。比如加密后的数据在传输过程中被黑客或恶意用户破解，并通过一定的工具修改了密文中的有关数值或信息，数据接收者如果无法校对数据的完整性，会将错误数据进行处理。为解决上述问题，通常会使用数据签名或散列函数对密文进行保护。

3. 可用性

数据可用性是一种以使用者为中心的设计概念，可用性设计的重点在于让产品的设计能够符合使用者的习惯与要求，也就是在确保数据保密性和完整性的同时，也要确保数据可以被使用者方便使用，而不能一味强调保密和完整而忽视数据存在的根本意义是被使用和处理。

19.2 数据生命周期

数据安全问题涉及数据整个生命周期的管理过程，即从创建到失去商业价值或按规定要求被删除。对银行而言，所有的数据在其生命周期中都应当被有效地管理，通过必要的控制手段清晰的界定，以使其避免内部非授权的访问。

数据的生命周期也叫信息的生命周期，一般由创建、保护、访问、迁移、归档、回收/销毁等六阶段组成，这六阶段的数据活跃度和相关手段如图 19-1 所示。

数据的安全当然需要在生命周期的各个阶段进行保护，数据安全并不单独存在，在

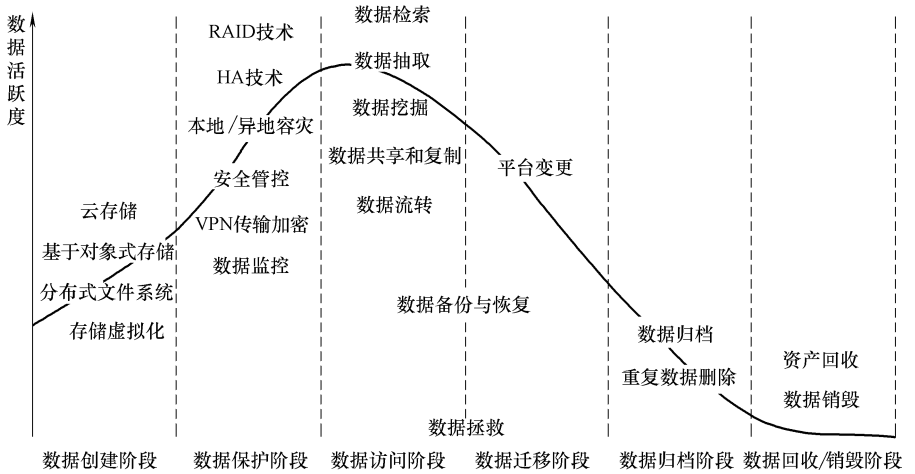


图 19-1 数据生命周期

物理安全、网络安全、主机安全、应用安全等各个阶段的安全措施都是对数据安全的支撑，在本章重点介绍数据层面的一些防护技术。

19.3 数据安全技术

19.3.1 数据加密技术

加密是保证数据安全的最核心的手段，在 18 章已经详细介绍了密码技术及密码技术在安全上起的作用，本节就不再展开讨论。

加密的基本功能包括：防止未授权者查看机密的数据文件；防止机密数据被泄露或篡改；防止特权用户（如系统管理员）查看私人数据文件；使入侵者不能轻易地查找一个系统的文件。

此外，数据加密也是确保计算机通信安全的一种重要机制。数据加密可在网络 OSI 七层协议的多层上实现，从加密技术应用的逻辑位置看，有 3 种方式：

（1）链路加密 通常把网络层以下的加密叫链路加密，主要用于保护通信节点未传输的数据，加解密由置于线路上的密码设备实现。

（2）节点加密 是对链路加密的改进。在协议传输层上进行加密，主要是对源节点和目标节点之间传输数据进行加密保护，与链路加密类似，只是加密算法要结合在依附于节点的加密模件中，克服了链路加密在节点处易遭非法存取的缺点。

（3）端对端加密 网络层以上的加密称为端对端加密，是面向网络层主体。对应用层的数据信息进行加密，易于用软件实现，且成本低，但密钥管理问题困难，主要适合大型网络系统中信息在多个发方和收方之间传输的情况。

19.3.2 数据存储安全技术

服务器中存储的信息是越来越多，而且也越来越重要。为防止服务器受到意外攻击，而导致大量重要的生产业务数据丢失，服务器一般都会采用许多重要的安全保护技术来确保服务器的安全。

1. 自动全备份技术

该技术是在网络系统上建立起的两套同样的且同步工作的服务器，如果其中一个出现故障，另一个将立即自动投入系统，接替发生故障的文件服务器的全部工作。使用该技术，可以确保容错系统的数据信息由于系统或人为误操作造成损坏或丢失后，能及时在本地实现数据的快速恢复能力；另外，该技术还可以确保容错系统在发生不可预料或者抵御的地域性灾难（地震、火灾、机器毁坏等）时，及时在本地或异地实现数据及整个系统的灾难恢复。

2. 事务跟踪技术

该技术是针对数据库和多用户软件的需要而设计的，用以保证数据库和多用户应用软件在全部处理工作还没有结束时或工作站或服务器发生突然损坏的情况下，能够保持数据的一致。其工作方式是对指定的事务（操作）要么一次完成，要么什么操作也不进行。

3. 自动检验技术

一般来说，在对错误的或者被损坏的数据进行恢复之前，该系统必须要有能力来及时发现这些引起错误的原因，所以一个完整的容错系统应该离不开自动检验技术的支持。自动检验技术是用于故障快速检测的一种有效手段，特别是具有完全自校验性质的自校验装置，它不仅能及时检查出系统模块的差错，还能够检测出自身的差错。在设计一个容错系统时，如果正确地使用自动检验技术，可以大大提高系统对差错的反应能力，使差错的潜伏期缩短，能有效地放置错误的进一步蔓延，从而有利于其他技术及时对错误做出相关的措施。

19.4 数据防泄密技术（DLP）

1. DLP 解决方案的类型与防护目标

（1）DLP 解决方案的类型 数据泄漏防护（Data Leakage Prevention，DLP）指的是用于监控、发现和保护数据的一组新技术。数据泄漏防护又称为数据泄密防护、数据防泄密技术。目前各种 DLP 解决方案，通常分为 3 种类型：

1）网络 DLP：通过假设网络设备于主要网络边界之间，最常见的是企业网络和互联网之间，像一个数据网关。网络 DLP 监控通过网关的流量，检测敏感数据或者与之相关的事情，发现异常时，阻止数据离开网络。

2）存储 DLP：通过软件运行在一台设备上或直接运行在文件服务器上，执行类似网络 DLP 的功能。存储 DLP 扫描存储系统寻找敏感数据。发现异常时，可以删除、隔离数据或通知管理员。

3）终端 DLP：软件运行在终端系统上监控操作系统活动和应用程序，观察内存和网络流量，以检测使用不当的敏感信息。

（2）DLP 的防护目标 网络 DLP、存储 DLP 和终端 DLP 都有相当的防护作用，也有各自的局限性，最终的解决方案经常是混合使用，来满足以下部分或全部目标：

1）监控：被动监控，报告网络流量和其他信息通信通道，如将文件复制到附加的存储。

2）发现：扫描本地或远程数据存储，对数据存储或终端上的信息进行分类。

3）捕获：捕获异常情况，并存储，以便事后分析和分类，或优化策略。

4）防护/阻塞：根据监控和发现组件的信息，阻止数据传输，或者通过中断网络会话或中断本地代理与计算机交互来阻断信息流。

DLP 解决方案需要混合以上技术，还需要管理配置策略集中服务器，来定义哪些数据需要保护及如何保护。

2. DLP 解决方案所面临的挑战

在实际业务中，如果 DLP 解决方案没有监控到特定的存储设备或网段，或者某种特定的文件没有关联合适的策略，DLP 解决方案便不能执行正确的保护，这意味着 DLP 技术的组件必须覆盖每个网段文件服务器、每个内容管理系统和每个备份系统，这显然不是容易的事情。另外，配置 DLP 环境和策略是项艰巨的任务，忽视任何一个方面，都可能会导致整体 DLP 解决方案的失效。

DLP 仅仅做时间点的决策。例如，一开始，DLP 允许用户发送机密数据给信任的合作伙伴，但 6 个月以后，该组织觉得合作伙伴太贵，转而与其他更便宜的合作伙伴签了协议。然后，重新配置 DLP 策略来响应业务关系的变化，但是 DLP 解决方案没有能力影响所有已经发给旧业务伙伴的信息。此时数据驻留在合作伙伴那里，而他可能将很快与你的竞争对手签订协议。

DLP 解决方案对于处理违规策略的方法是有局限的，但有时这种防护会干扰整个业务。例如，当用户复制文件或者电子邮件时，DLP 解决方案阻止复制它，因为这是不合法的。可有一天，CEO 在做一个重要的宣讲，并想要将文件复制到一个没有加密的 USB 设备中，将营销报告分享给董事会，会怎么样呢？DLP 可能会阻止他。如果想要通过电子邮件向自己的私人邮箱发送一个重要文档，在周末加班时用，又会怎么样呢？不行，DLP 会阻止它并通知 IT 安全团队，虽然 DLP 中有很多优势，但如果不考虑所有可能的场景，就很有可能会影响业务流程和生产。

DLP 也会生成一定数量的误报（和漏报），这使得完全执行所有阻止/防护组件是一个危险的动作。即使执行策略的准确性非常高，组织也会经常发现业务中断率很高，所以他们更喜欢只采取实现监控。

尽管 DLP 有一些不足，但 DLP 在抓获和监控敏感数据的移动方面仍然是一个非常好的工具，它能透视网络中的信息流。这非常有价值，至少，可以突出显示非法活动发生或者敏感信息存储在开放共享的文件中。DLP 网络监控和发现组件的报告提供了一个有用的反馈环路：标识符合“热点”及不良的工作方法，映射敏感内容到整个组织，并使组织可以调整现有的访问控制系统。

19.5 案例介绍：数据防泄密技术在银行的实践

19.5.1 数据安全分析

1. 银行数据使用的典型场景

（1）终端数据的使用及存储 行内员工使用 PC 终端或者笔记本电脑办公，处理业

务工作，接收、发送企业内部的通信信息，接收其他部门发送的内部资料，在使用或者编辑完这些资料后，一般会存储在 PC 终端、笔记本、移动存储设备或者提交到相关应用系统。

员工通过 PC 终端或者笔记本通过网络认证准入后，直接访问办公系统（OA、CRM 等）或者高敏感的业务系统，在线处理系统中的业务工作流，如果工作需要，还可以下载资料附件或者业务数据（财务数据、分析数据等）到终端离线办公，完成后再回传到业务系统中（图 19-2）。

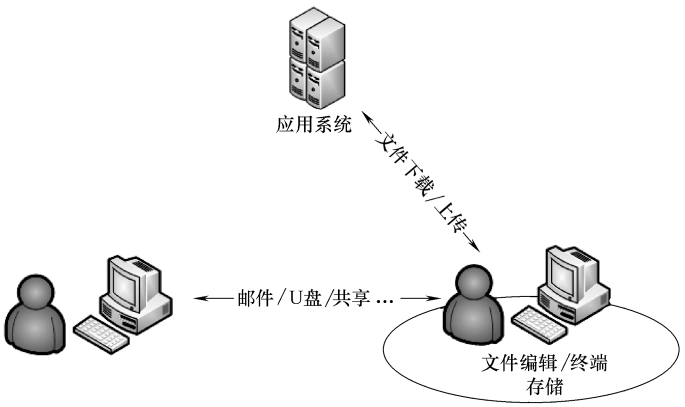


图 19-2　银行数据使用场景

（2）敏感文件内部传输　在一些特定场景下，员工需要将一份含有敏感信息的文件（合同、人事任命、财务报表等）发送给指定人员或者领导，由于文件信息较为敏感，因此一般通过邮件、内部即时通信系统或者使用普通 U 盘拷贝给指定人员，保证文件安全传递给合法的使用者。但是由于没有统一的安全标准，各个部门的处理方式千差万别，并且在大部分时候没有采取任何技术保障措施，完全是由员工自行保护敏感文件。

（3）敏感文件外发信息交互　市场部门、业务部门、商务部门等对外部门，经常会将企业内部文件，如合同文件、采购标准等企业信息外发给合作伙伴或者上级单位，双方频繁的文件交互缺乏技术手段保护外发文件，文件接收方可以随意处理这些信息打印、外发甚至是发送到互联网论坛。

（4）企业信息发布资源分享　在实际工作当中，各个部门（如人事部门、市场部门、财务等）或者集团总部经常会给本部门或者分公司群发通知性邮件，除了邮件正文还包括附件信息，有时由于邮件系统群发邮件发送量过大，尤其是群发包含大附件的文件的时候，接收缓慢，占用带宽，甚至影响到了员工的工作效率。

（5）终端访问互联网　行内员工在日常的办公过程中，需要访问到互联网进行一些资料的查阅和各种互联网业务的办理。同时，该终端也会具备权限访问内部的一些办公系统甚至敏感的数据。访问互联网的终端也存在内部的敏感数据，终端任何数据都可通过互联网进行传输。

（6）终端访问敏感应用系统 行内员工、三方运维人员、出差人员需要访问内部应用系统，当终端允许网络准入或通过 VPN 接入到内网应用后，用户可以在线编辑、处理业务系统数据，文件在线查看，甚至下载敏感文件、系统日志文件到终端，离线办公，访问敏感资源（应用系统）的时候未对终端进行检测并且控制终端状态，下载的敏感数据与个人数据混合存储在终端。

2. 面临的数据安全风险

根据行内信息化现状，已经采取的安全措施，针对数据安全现状风险，从以下几个方面进行阐述。

（1）数据存储风险

1）终端设备丢失造成泄密。由于员工在实际工作当中，会接触到很多的敏感办公文件，包括员工自己产生的文档，或者从各种应用系统中下载的办公文件，由于文件中包含敏感信息，需要加强保护。而在实际使用过程中，没有采取任何的安全措施或者保护手段，分散存储在各个办公终端中，如 U 盘、移动硬盘、笔记本等。例如，出差的时候会在笔记本中存储很多的敏感文件，如果笔记本丢失或者被盗，由于笔记本除了系统登录密码外，没有任何的保护手段，极易造成数据泄密，甚至造成不良的社会影响。

2）终端分散存储造成风险。终端上分散存储着大量文档，如果终端系统崩溃或应用办公文件故障导致文件损坏，由于没有采取任何备份措施，必然影响到日常办公，分散存储不仅给个人文档管理带来风险，同时也给内部的知识传递和分享造成瓶颈。

3）终端联网数据被动泄密风险。由于互联网是一个开放的网络，存在众多的不确定性安全风险。特别是当终端连接互联网的时候，互联网的威胁可能引入到终端上。而终端本身的数据存在被动或者主动传输到互联网上的风险，从而造成终端数据泄露的安全隐患。

（2）内部使用风险 业务数据和客户数据是行内的核心资产，直接关系着企业的核心竞争力，由于内部之间都是采用明文的方式进行传输，随着文档在内部扩散，在内部不仅存在一般性质的文件传递及资料分享，有的还包括较为敏感的文件如商务合同、财务报表、薪酬文件等，这类文件需要严格控制阅读人员及阅读范围的资料，而现阶段只是做了安全规章制度的要求，如果文件接收者有意外发文件或者打印敏感文件，必然造成文档在内部使用风险。

（3）文件管理风险 信息安全建设过程中，对内部的信息安全已起到了一定的安全保障，但是对内部的信息流转、文档分布依然缺乏有效的管理，缺乏对内部文档的统一管理，包括文档操作记录、文档分布状态、违规使用记录等，各信息安全管理系统之间缺少信息的联动，使得内部对文档的管理存在风险。

（4）外部使用风险 由于业务需要，经常需要将内部的文件外发给第三方合作伙伴或客户，但是部分外发信息较为敏感，如果这些文件在外部网络被截取，或者接收者保管不善，造成文件内容泄密，将影响到行内的业务甚至是企业形象，甚至影响业务的

顺利进行。

（5）内部流转风险 文档在内部流转过程中，可能存在越权查看或恶意传播的风险，如某些敏感文件只能限定在某些范围内查看的文件，但是在实际工作中，可能存在越权查看、非法传播，甚至还存在恶意传播的风险。

（6）占用带宽造成网络拥堵 内部数据传输的时候，通常使用共享、邮件等用于内部信息分享和传递，如果是文字性的内容，内部通信既可靠又保证通信顺畅，但是在实际使用的时候，员工会将文件或者较大的文件以附件的形式分发出去，直接发送的邮件服务器，这个时候接收者会收到邮件信息，手动或者自动同时下载文件，从而造成网络拥堵，占用大量带宽，影响到其他应用系统的网络通信，甚至是影响企业运行效率，造成经济损失。

19.5.2 安全桌面功能框架

安全桌面的主要功能包括安全桌面终端防护、透明接入、本地数据加密、安全桌面时间计划、防粘贴拷贝、防泄密水印、插件/证书白名单、防二次跳转、安全桌面离线使用、访问策略控制、认证授权、传输安全、安全桌面多实例和个性化、应用白名单、软件兼容性、安全桌面与真实桌面之间数据安全交换、上网桌面和办公桌面同时使用、操作系统兼容、日志审计的功能（表 19-1）。

表 19-1 具体功能列表

功能类型	功能需求说明
安全桌面终端防护	1. 在网关配置屏蔽沙盒内的任务管理器、关机、注销、控制面板、注册表、运行菜单 2. 终端健康性检查，包括操作系统版本号、补丁（只检查 SP1/SP2 等大版本）、检查防病毒软件是否安装/病毒库是否过期、检查防火墙是否安装等 3. 对外设进行管控，管控打印机、COM 口、USB 口的使用，尤其对 USB 介质在禁止 USB 存储设备的同时，可以允许网银 USB Key 及 USB 鼠标、键盘使用 4. 安全桌面支持防截屏/录像能力
透明接入	不改变用户物理 IP 地址，不需安装虚拟网卡，对用户透明方式来建立安全隧道，并接入安全桌面网关，进而访问网络；不影响原有的上网审计（仍可基于 IP 进行管控）
本地数据加密	安全桌面对本地数据进行加密存储，不同策略安全桌面文件加密采用独立密钥。同一计算机的不同用户的不同策略安全桌面数据不能相互读取；同一计算机的同一用户的不同策略安全桌面数据（敏感、互联网）不能相互读取
安全桌面时间计划	支持用户使用安全桌面时间控制管理，能够对不同用户或角色分配不同的时间计划，确保用户对互联网和敏感资源的合理使用。为不改变现有用户使用模式，时间计划控制由分行根据实际情况选择是否开启
防粘贴板拷贝	使用对系统粘贴板拷贝的方法，也可能导致关键信息的泄漏，在安全桌面内通过屏蔽安全桌面粘贴板等措施，防止机密数据泄露。该功能在网关配置中开启
防泄密水印	安全桌面具有水印配置功能。安全桌面显示水印，水印内容包括用户名、登录网关等，防范通过截图、拍照等操作造成信息泄露

（续）

功能类型	功能需求说明
插件/证书白名单	由于沙盒原理实现上，在启用退出清空策略后不保存沙盒内的任何操作，包括沙盒内安装的 IE 插件、证书；安全桌面内制订白名单允许沙盒内匹配白名单的插件、证书安装并保留，以避免每次需要重新安装插件。白名单默认包含主流 IE 插件及网银证书，并根据需要在网关侧手动维护列表
防二次跳转	安全桌面具备防二次跳转能力，防止其他非授权终端通过远程桌面功能跳转到启动安全桌面的终端上，从而达到非法上网的目的。该功能在网关配置中开启
安全桌面离线使用	在安全桌面离线时，不能访问任何敏感信息资源，可以访问安全桌面本地资源。互联网安全桌面不允许离线运行，防止在非受控情况下访问互联网
访问策略控制	安全网关部署完成后，不启动安全桌面客户端的电脑无法直接访问互联网和敏感资源服务器。启动安全桌面客户端后，对真实桌面及安全桌面分别下发网络访问控制策略，限制真实桌面及安全桌面的访问网段，确保用户只能访问授权的网络资源
认证授权	支持 AD 域、Radius 认证、证书认证，能控制用户访问的网络系统权限，实现针对不同用户、用户组进行访问权限的管理
传输安全	安全桌面与网络资源的通讯应采用加密传输方式，并支持中国商密算法 SM1 等
安全桌面多实例和个性化	支持多个安全桌面同时运行，支持悬浮提示条可以在安全桌面与本地桌面之间快速切换；能自定义和统一定义桌面壁纸，避免多个桌面同时启用时使用混淆
应用白名单	可对安全桌面内运行的程序进行管理，仅允许白名单内的应用运行
软件兼容性	支持的应用包括但不限于以下内容（后续会增加新应用）： iNode 和时代亿信文档加密软件 办公软件：Office 阅读软件：Adobe Reader 输入法：搜狗拼音输入法、搜狗五笔输入法 视频软件：暴风影音、Adobe Flash Player 压缩软件：WinRAR 安全软件：杀毒软件、防火墙 浏览器：IE 6 以上全部版本，Chrome、Firefox 指定版本 翻译软件：金山词霸 聊天软件：QQ、飞信、Skype 行内软件和网银控件
安全桌面与真实桌面之间数据安全交换	安全桌面与真实桌面之间进行文件导入、导出时可对文件内容进行指纹级审计，基于敏感关键字阻断或进行审计，记录传输文件名、用户名、来源 IP、MD5 及文件指纹片段；文件导出/导入失败时，提示用户失败及原因，并记录违规日志；对导出/导入文件能自动保存审计
上网桌面和办公桌面同时使用	一个安全桌面网关可以同时支持上网桌面和办公桌面使用
操作系统兼容性	支持 Windows XP、Win7/Win8/ Win2008（32 位和 64 位）
日志审计	支持对安全桌面内网络资源访问进行细粒度审计和日志记录，日志包括登录用户、访问时间、源地址、目的地址等，并支持外部标准 SYSLOG 服务器日志输出

19.5.3 安全桌面技术说明

在政府、金融等单位中，用户在工作时既需要访问互联网，又需要访问内部的专网。由于内部业务系统中传输的都是内部机密的信息，用户在上网过程中有意或者无意的把内部的文件发送到互联网上，这种行为就是网络泄密。从有意和无意两个角度来分，网络泄密可以分为主动泄密和被动泄密。主动泄密的方式主要包含通过发帖、外发邮件、QQ 聊天、USB 拷贝把单位的机密文件发送出去；被动泄密主要是用户在中了病毒或木马后，病毒程序通过扫描用户电脑，把有用的资料偷发出去，或者利用被中毒的 PC 作为跳板，访问内部的服务器，从服务器上获取资料再发送出去。无论是哪种泄密方式，给单位和企业都会带来巨大的经济损失。所以在政府、金融等单位，需要通过技术手段来实现互联网和内网隔离，防范信息泄密风险。

当前有两种主流的技术方案，一种为物理隔离，即每个用户使用两台 PC，一台上网，一台办公；另一种为逻辑隔离，即安全桌面技术，通过在 PC 上虚拟一个安全的桌面环境，实现互联网和办公的逻辑隔离。物理隔离投资大，易用性差，正在逐渐被替代。当前安全桌面技术已经被一些银行大规模采用，方案成熟可靠。

针对物理隔离和安全桌面（逻辑隔离）的详细对比，见表 19-2。

表 19-2 物理隔离与安全桌面对比

	项目	物理隔离	安全桌面(逻辑隔离)
建设投资	建设投资	两套物理网络、两套布线、两套终端设备	一套物理设备、一套虚拟系统组成
	建设周期	长	短;确定方案,1 个月以内就能完成实施和调试
业务可行性	实际隔离实现	无法兼顾业务的使用性,无法真正实现完全隔离	兼顾业务的实际操作系统,隔离效果可控制、可调节
维护和管理	网络管理性	两倍管理成本	易管理,仅需通过安全桌面网关设备进行统一管理
	维护成本	高	低;只需要维护安全桌面网关即可
易用性	用户操作性	差,必须换设备进行操作,影响工作效率	好,进行安全桌面切换操作即可;不影响操作习惯
方案扩展性	性能扩展性	较差;扩展新增设备必须同时增加两套	利用安全桌面网关的集群功能,可以达到极佳的扩展性

安全桌面产品采用了沙盒技术和安全桌面技术，具体内容如下。

1. 沙盒技术

Sandbox 技术，中文名叫沙盒，也叫沙箱、沙盘。在计算机领域指一种虚拟技术，且多用于计算机安全技术。其原理是提供一个虚拟的环境给程序运行，当发现程序有破坏行为的时候，终止该进程。由于程序是在虚拟的环境中执行的，所造成的破坏也不会影响到真实环境中。想象一下，在一个装满了平整细沙的盒子里，我们可以尽情随意地在上面作画、涂写，无论画得好坏，最后轻轻一抹，沙盒又回到了原来的平整状态。

目前，沙盒技术已经成为安全界一种流行的技术来解决终端安全问题。众多知名厂商都在各自的产品、不同领域使用沙盒技术来提升产品的安全性。比如苹果的 iOS 系统，采用沙盒技术后，iPhone、iPad 的安全性得到很大提升，恶意代码远低于安卓系统；谷歌的 Chrome 浏览器，采用沙盒技术后，Chrome 对恶意代码的防护效果得到极大提升，被评为安全浏览器。

2. 安全桌面技术

安全桌面是使用了 SandBox 技术的一种安全逻辑隔离产品，也是虚拟化技术的一种应用。互联网场景下使用安全桌面既可用于病毒防护，也可以用于数据防泄漏。安全桌面使用的关键技术有以下几种。

（1）调用拦截 通过 windows 的图形化进程管理器 explorer. exe，安全桌面下发控件后，在终端生成一个新系统进程管理器，在新系统进程管理器下面再次调用其他的程序和使用的文件，并对数据传输、I/O 系统、DLL 代码数据库、进程间通信接口 API 等进行数据调用拦截。

（2）重定向 通过 HOOK 技术，对安全桌面下的所有运行的程序，都将受到沙盒相关进程的改写，实现与原有环境的隔离。

（3）透明访问 采用系统级网络拦截技术，将用户的 IP 数据包自动增加标记，发送到安全桌面网关，网关解开后仍然可以使用用户的物理 IP 将访问请求发出，不影响记录日志和基于源 IP 的审计追溯。

（4）透明加密技术 用户在安全桌面中进行网络访问、本地文件访问等操作时，可自动将保存在安全桌面中的数据加密，用户无感知。

（5）注册表保护 安全桌面内被修改过的注册表单被重新定向到加密注册表中，安全桌面无法看到，关闭安全桌面后，该注册表单被恢复或删除。通过注册表保护，可以避免病毒感染、修改注册表键值。

（6）进程保护 通过进程访问控制，防止病毒感染虚拟环境以外的进程，当用户退出安全桌面后，所有的病毒数据文件都将被清除，以保护系统进程安全，避免被病毒感染。

（7）网络访问控制 安全桌面中可根据设置的网络访问规则，分别对真实桌面和安全桌面内的网络访问进行控制。

19.5.4 防数据泄漏平台介绍

1. 平台介绍（图 19-3）

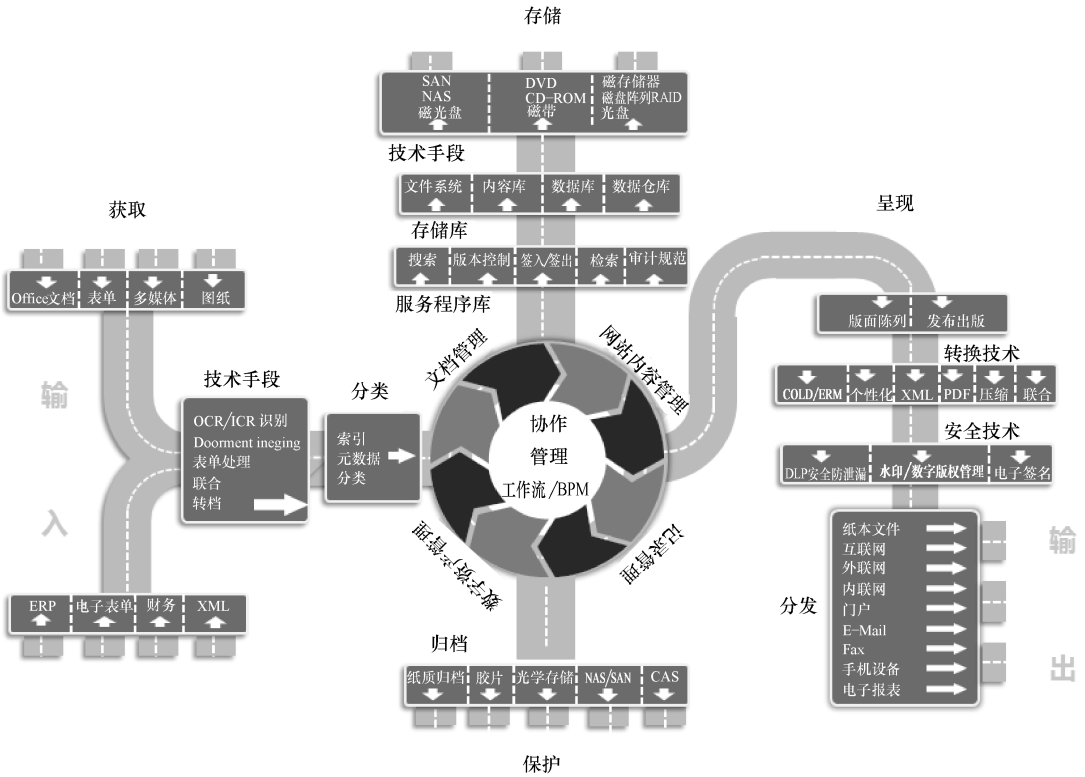


图 19-3 平台示意图

（1）获取 提供多种方式将文件获取至系统，如单/多个文件（夹）、第三方集成、扫描件、移动终端采集、同步、Office 组件集成等。

（2）存储 提供高效、安全、可扩展的存储方式，分区域存储加速文件访问速度。

（3）管理 对文件提供一系列的管理方式，分别为文档管理、网站管理、记录管理、数字资产管理。

（4）保护 对文件提供全方位的权限保护机制。

（5）呈现 以门户、预览、知识地图等方式将信息展示给用户。

2. 功能架构（图 19-4）

（1）用户层 提供多种访问方式，如利用网页、客户端、一体机等方式访问系统。

（2）内容应用层 在文件采集、存储、内容组织、内容发现、共享协作、内容业务等方面进行应用。

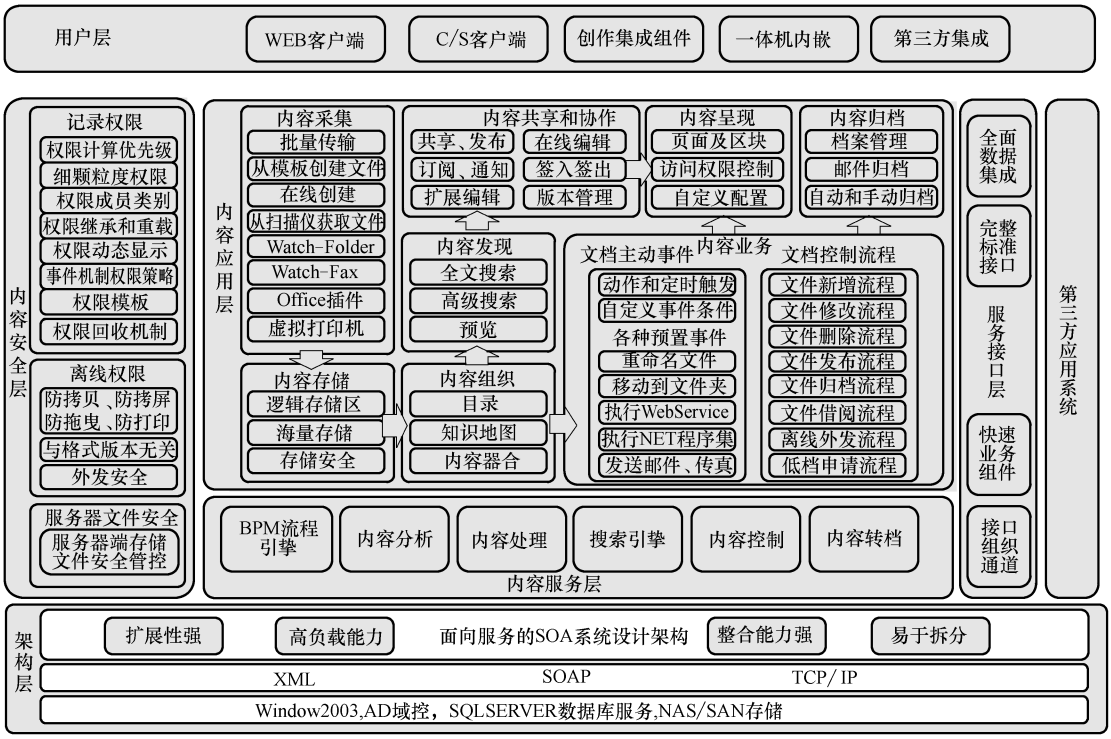


图 19-4　功能构架图

（3）内容安全层　提供在线权限分配体系，使权限颗粒化，保证文件的在线安全，并提供离线权限，以保证文件外发后的安全性。

（4）内容服务层　系统提供多种服务，如搜索服务、转档服务器、内容分析服务，并提供多种报表监控系统运行情况。

（5）架构层　系统采用 SOA 架构，具备较强的扩展性、高负载能力、较强的整合能力，并且易于拆分，方便快速整合。

（6）第三方集成　提供标准 Web Service，方便与第三方系统快速整合，包括数据集成、业务组件集成、组织集成等。

第 20 章
安全检测与渗透测试技术

20.1 系统安全检测及渗透技术

20.1.1 系统安全检测方法概述

近年来，随着网络攻击技术的泛滥，不少企业的信息系统会经常遭到黑客的攻击和信息的篡改，针对网络信息系统攻击的各种犯罪活动已经严重危害着社会的发展和企业的安全，给全球带来了巨大的经济损失。总之，当前信息系统所面临的各种各样的威胁问题，已经成为普遍的国际性问题。

信息革命在改变人类传统的生产、生活方式并极大地促进生产力发展的同时，也带来了不容忽视的负面影响。信息系统的安全正成为每一个计算机用户都面临的紧迫问题。为了解决这些问题，一系列的网络安全技术应运而生。

1. 漏洞扫描

漏洞是指一个系统存在的弱点或缺陷，即系统对特定威胁攻击或危险事件的敏感性，或进行攻击的威胁作用的可能性。漏洞可能来自应用软件或操作系统设计时的缺陷或编码时产生的错误，也可能来自业务交互处理过程中的设计缺陷或逻辑流程上的不合理之处。这些缺陷、错误或不合理之处可能被有意或无意地利用，从而对一个组织的资产或运行造成不利影响，如信息系统被攻击或控制，重要资料被窃取，用户数据被篡改，系统被作为入侵其他主机系统的跳板。从目前发现的漏洞来看，应用软件中的漏洞远远多于操作系统中的漏洞，特别是 WEB 应用系统中的漏洞更是占信息系统漏洞中的绝大多数。

漏洞会影响到很大范围的软硬件设备，包括系统本身及其支撑软件、网络客户和服务器软件、网络路由器和安全防火墙等。换而言之，在这些不同的软硬件设备中都可能

存在不同的安全漏洞问题。在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

每个系统都有漏洞，不论你在系统安全性上投入多少财力，攻击者仍然可以发现一些可利用的特征和配置缺陷。这对于安全管理员来说，实在是个不利的消息。但是，多数的攻击者，通常做的是简单的事情。发现一个已知的漏洞，远比发现一个未知漏洞要容易得多，这就意味着多数攻击者所利用的都是常见的漏洞，这些漏洞，均有书面资料记载。这样的话，采用适当的工具，就能在黑客利用这些常见漏洞之前，查出网络的薄弱之处。如何快速简便地发现这些漏洞，这个非常重要。漏洞，大体上分为两大类：

1）软件编写错误造成的漏洞。

2）软件配置不当造成的漏洞。

漏洞扫描就是对重要计算机信息系统进行检查，发现其中可被黑客利用的漏洞。漏洞扫描的结果实际上就是系统安全性能的一个评估，它指出了哪些攻击是可能的，因此成为安全方案的一个重要组成部分。

目前，漏洞扫描，从底层技术方面来划分，可以分为基于网络的扫描和基于主机的扫描这两种类型。

后面会分别介绍并分析基于网络的漏洞扫描工具和基于主机的漏洞扫描工具的工作原理。这两种工具扫描目标系统漏洞的原理类似，但体系结构是不一样的，具有各自的特点和不足之处。

2. 源代码扫描

信息安全是一个随时都在发展和变化的动态事物，攻击的领域已经由传统的网络和系统层面上升到了应用层面。近期，越来越多的应用系统面临着攻击威胁。应用系统的安全性能，一方面立足于系统安全方案的分析与设计，另一方面也取决于系统实现过程中是否存在安全性缺陷。为降低应用系统的安全风险，减少软件代码编写中可能出现的安全漏洞，提高应用系统自身安全防护能力，软件的应用方越来越依赖于采用源代码安全扫描工具在软件开发过程中帮助软件开发团队快速查找、定位、修复和管理软件代码安全问题，应用静态源代码安全扫描的主要价值在于能够快速准确地查找、定位和修复软代码中存在的安全风险，增加工具投资所带来的最大效益，节约代码安全分析的成本，最终开发安全的、可靠的软件。

静态源代码扫描的优点在于，无须进行编译，也无须去搭建运行环境，就可以对程序员所写的源代码进行扫描。这样可以节省大量的人力和时间成本，提高开发效率，并且能够发现很多靠人力无法发现的安全漏洞，站在黑客的角度上去审查程序员的代码，大大降低项目中的安全风险，提高软件质量。

在静态源代码扫描技术上，现在被普遍应用的是第一代和第二代技术。

第一代技术是指传统的静态分析，都是基于语法解析或者编译器，这些方式分析代码的缺陷是以代码所匹配的规则模式（patterns）去评估代码，只要模式匹配或者相似就报出来。需要人工去分辨出其中的真假，主要存在的问题是误报（False Positive）和

漏报（False Negative）。

出现这两个问题的原因是：在做静态分析时，要先描绘出代码所有的路径，然后对每种路径上的变量进行计算，并比较。基于语法的解析路径是可以描绘出来的，但要计算每个路径上的变量在使用前后的值，并跟踪它们，目前采用的算法几乎不可能，就是上面的程序也要花费相当长的时间，几乎无法接受。因此目前许多静态工具只是把感染的路径找到，但不计算和不做比较，需要借助人工去分辨所有可能的情况，这就是它们误报率非常高的原因。

在小量的代码前提下，简单的代码将不是问题，也是可以接受的。但是，如果是大量的代码、复杂的代码，传统的扫描技术几乎不可行，因为它将大量浪费开发和安全审计人员的时间，有时人眼也无能为力。

近期，美国和以色列的一些技术人员又提出了一种新的代码扫描技术，也称之为第二代的静态源代码扫描技术。

这种技术可简单地理解为，把代码劈开，把待分析的代码及代码之间的关系以对象的方式存放在内存中，同时也使用了一种可以接受的算法在有效的时间里描绘出应用的路径图形，并采用了一种特殊的查询语言 CxQL 来查找安全问题，每一个查询语句就针对一类安全漏洞问题，因此几乎可以达到完美的结果，从而消除了误报。用户可以利用 CxQL 语言定制自己的查询语句（规则），查找特定的安全和逻辑的问题，解决漏报问题，使得代码扫描变得更加现实和可用；也可以给项目开发节省大量的时间和人力成本，大大提升软件的安全性能。

3. 安全配置核查

安全配置顾名思义，是指设备自身的安全策略、安全运行参数等一系列安全指标合集，额外还包含部署在此设备上的支撑软件（如数据库、中间件）的安全指标。安全配置是保持设备系统在机密性、完整性、可靠性需求上的最小安全控制。因此通过确保能满足安全配置的要求，从而保证设备及业务的正常运行，并从中得到了最低程度的安全保证，其重要性不言而喻。

目前我国安全配置的标准主要是依据等级保护（1～5 级）和分级保护（秘密/机密/绝密），而具体落实和操作由 GB/T 和 BMB 打头的相关标准来实现。其主要文件是《信息安全技术信息系统安全等级保护基本要求》和《信息安全技术信息系统安全保护等级定级指南》。上述两个方面的标准由于存在内容分散、相互抵制等问题，在实际操作中难以实现，因此需要寻找一种更为高效、准确的核查方法。针对上述情况，2014 年 6 月，中央网络安全和信息化领导小组办公室（中央网信办）颁布了《2014 年国家网络安全检查工作方案中网办发（2014）5 号》和《国家网络安全检查操作指南（附 5 号文）》，明确了网络安全检查的内容，其中就包含了配置核查的内容。

4. 渗透测试

渗透测试（Penetration Test）并没有一个标准的定义，国外一些安全组织达成共识的通用说法是：渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全

的一种方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，是从一个攻击者可能存在的位置来进行分析的，并且从这个位置有条件地主动利用安全漏洞。

渗透测试还具有的两个显著特点是：渗透测试是一个渐进的并且逐步深入的过程；渗透测试是选择不影响业务系统正常运行的攻击方法而进行的测试。作为网络安全防范的一种新技术，对于网络安全组织具有实际应用价值。

渗透测试是一种最老的评估计算机系统安全性的方法。在 20 世纪 70 年代初期，国防部就曾用这种方法发现了计算机系统的安全漏洞，并促使开发构建更安全系统的程序。渗透测试越来越多地被许多组织用来保证信息系统和服务的安全性，从而使安全性漏洞在暴露之前就被修复。由于恶意代码、黑客、不满员工所造成的网络入侵、数据偷窃和攻击的频率和严重程度会继续增加，所以网络安全漏洞和数据偷窃所造成的风险和代价是极大的。由于企业电子化的兴起及其对安全性的要求，公司网络的远程访问也在增加。事实上，即使网络实现管理的很好，并使用了最新的硬件和软件，也仍然可能受到错误配置或软件缺陷的影响。这可能最终会将敏感信息的访问权限泄漏给入侵者。虽然渗透测试的主要目标是发现组织中网络基础架构的安全漏洞，但它也可能有许多次要目标，包括测试组织的安全问题识别和响应能力，测试员工安全知识或安全性政策规范等。

20.1.2 主流检测技术介绍

1. 漏洞扫描技术

漏洞扫描技术是一项重要的主动防范安全技术。非法入侵者的攻击行动主要是利用各种网络漏洞侵入，使防火墙类设施形同虚设。漏洞扫描器是自动检测远程或本地主机安全性弱点的程序。通过使用漏洞扫描器，发现所维护的 WEB 服务器的各种 TCP 端口的分配、提供的服务、WEB 服务软件版本和这些服务及软件呈现在 Internet 上的安全漏洞，从而在计算机网络系统安全保卫战中做到“有的放矢”，及时修补漏洞，就可以有效地阻止入侵事件的发生，从而构筑坚固的安全防线。

（1）基于网络的漏洞扫描 基于网络的漏洞扫描器，就是通过网络来扫描远程计算机中的漏洞。比如利用低版本的 DNS Bind 漏洞，攻击者能够获取 root 权限侵入系统，或者攻击者能够在远程计算机中执行恶意代码。使用基于网络的漏洞扫描器，能够监测到这些低版本的 DNS Bind 是否在运行。

一般来说，基于网络的漏洞扫描器可以看作一种漏洞信息收集工具，它根据不同漏洞的特性，构造网络数据包，发给网络中的一个或多个目标服务器，以判断某个特定的漏洞是否存在。

基于网络的漏洞扫描器包含网络映射（Network Mapping）和端口扫描功能，一般结合了 Nmap 网络端口扫描功能，常常用来检测目标系统中到底开放了哪些端口，并通过特定系统中提供的相关端口信息，增强了漏洞扫描器的功能。基于网络的漏洞扫描器，一般由以下几个方面组成。

1）漏洞数据库模块：漏洞数据库包含了各种操作系统的各种漏洞信息，以及如何检测漏洞的指令。由于新的漏洞会不断出现，该数据库需要经常更新，以便能够检测到新发现的漏洞。

2）用户配置控制台模块：用户配置控制台与安全管理员进行交互，用来设置要扫描的目标系统，以及扫描哪些漏洞。

3）扫描引擎模块：扫描引擎是扫描器的主要部件。根据用户配置控制台部分的相关设置，扫描引擎组装好相应的数据包，发送到目标系统，将接收到的目标系统的应答数据包，与漏洞数据库中的漏洞特征进行比较，来判断所选择的漏洞是否存在。

4）当前活动的扫描知识库模块：通过查看内存中的配置信息，该模块监控当前活动的扫描，将要扫描的漏洞的相关信息提供给扫描引擎，同时还接收扫描引擎返回的扫描结果。

5）结果存储器和报告生成工具：报告生成工具是利用当前活动扫描知识库中存储的扫描结果，生成扫描报告。扫描报告将告诉用户配置控制台设置了哪些选项，并且根据这些设置进行扫描后，在哪些目标系统上发现了哪些漏洞。

（2）基于主机的漏洞扫描 基于主机的漏洞扫描器，其扫描目标系统的漏洞的原理，与基于网络的漏洞扫描器的原理类似，但是，两者的体系结构不一样。基于主机的漏洞扫描器通常在目标系统上安装了一个代理（Agent）或者是服务（Services），以便能够访问所有的文件与进程，这也使基于主机的漏洞扫描器能够扫描更多的漏洞。现在流行的基于主机的漏洞扫描器在每个目标系统上都有个代理，以便向中央服务器反馈信息。中央服务器通过远程控制台进行管理。

基于主机的漏洞扫描器通常是一个基于主机的 Client/Server 三层体系结构的漏洞扫描工具。这三层分别为漏洞扫描器控制台、漏洞扫描器管理器和漏洞扫描器代理。

漏洞扫描器控制台安装在一台计算机中，漏洞扫描器管理器安装在企业网络中，所有的目标系统都需要安装漏洞扫描器代理。漏洞扫描器代理安装完后，需要向漏洞扫描器管理器注册。当漏洞扫描器代理收到漏洞扫描器管理器发来的扫描指令时，漏洞扫描器代理单独完成本目标系统的漏洞扫描任务；扫描结束后，漏洞扫描器代理将结果传给漏洞扫描器管理器，最终用户可以通过漏洞扫描器控制台浏览扫描报告。

2. 源代码扫描技术

随着市场竞争的日益激烈，以及通信与计算机技术的不断发展，业务支持系统的软件规模日益庞大，应用环境日益复杂，新业务需求层出不穷，旧业务不断更新优化；对系统源代码的质量要求也越来越高。从提高系统的安全性及稳定性出发必须进行源代码质量控制，保证源代码的质量，确保系统稳定高效的运行。

互联网的飞速发展，各种网络应用不断成熟，各种开发技术层出不穷，上网已经成为人们日常生活中的一个重要组成部分。在享受互联网带来的各种方便的同时，不断受到黑客、病毒、木马等各种攻击的安全问题也变得越来越重要。

根据信息技术研究与顾问咨询公司 Gartner 统计数据显示，75% 的黑客攻击发生在应用层；而由 NIST 统计显示，92% 的漏洞属于应用层而非网络层。因此，应用软件自

身的安全问题是信息安全领域最为关心的问题，也是面临的一个新的领域，需要所有在应用软件开发和管理的各个层面的成员共同的努力来完成。越来越多的安全产品厂商也已经在考虑关注软件开发的整个流程，将安全检测与监测融入需求分析、概要设计、详细设计、编码、测试等各个阶段以全面保证应用安全。

对于应用安全性的检测，目前大多数是通过测试的方式来实现。测试大体上分为黑盒测试和白盒测试两种。黑盒测试一般使用的是渗透的方法，这种方法仍然带有明显的黑盒测试本身的不足，需要大量的测试用例来进行覆盖，且测试完成后仍无法保证软件是否仍然存在风险。现在白盒测试中源代码扫描越来越成为一种流行的技术，使用源代码扫描产品对软件进行代码扫描，一方面可以找出潜在的风险，从内对软件进行检测，提高代码的安全性，另一方面也可以进一步提高代码的质量。黑盒的渗透测试和白盒的源代码扫描内外结合，可以使得软件的安全性得到很大程度的提高。

3. 渗透测试技术

渗透测试，是指为了对客户目标网络的安全性进行实际检查，进行带有攻击性行为的全面的安全压力测试。渗透测试是评估客户目标主机和网络的安全性时模仿黑客特定攻击行为的过程。详细地说，是指安全工程师尽可能完整地模拟黑客使用的漏洞发现技术和攻击手段，对客户目标网络的安全性进行深入的探测，发现系统最脆弱环节的过程。测试过程中，会采用各种手段和途径，包括端口扫描、漏洞扫描、密码猜测、密码破解、数据窃听、伪装欺骗等技术方式，最终目的就是为了检验该网络各个环节的安全性。

（1）信息收集技术 信息收集是每一步渗透攻击的前提，通过信息收集可以有针对性地制订模拟攻击测试计划，提高模拟攻击的成功率，同时可以有效地降低攻击测试对系统正常运行造成的不利影响。信息收集的方法包括 Ping Sweep、DNS Sweep、DNS zone transfer、操作系统指纹判别、应用判别、账号扫描、配置判别等。信息收集常用的工具包括商业网络安全漏洞扫描软件（如游刃、极光等）、免费安全检测工具（如 NMAP、NESSUS 等）。操作系统内置的许多功能（如 TELNET、NSLOOKUP、IE 等）也可以作为信息收集的有效工具。

渗透测试在实际进行中有以下两种不同的方法。

1）黑盒测试。黑盒测试又被称为“Zero-knowledge Testing”，渗透测试工程师完全处于对系统一无所知的状态，通常这类测试的最初信息来自于 DNS、WEB、E-Mail 及各种公开对外的服务器。

黑盒测试被称为功能测试或数据测试，在测试时，将被测软件视为一个不能打开的盒子，在完全不考虑程序内部结构和内部特性的情况下进行测试。采用黑盒测试的主要目的是在已有软件产品所应具有的功能等基础上进行下列操作：

① 检查程序功能是否按照需求规格说明书的要求正常使用，测试每个功能是否有遗漏，测试性能特性是否满足要求。

② 测试人机交互是否错误，检测数据结构或外部数据库访问是否错误，程序是否能适当地输入数据而产生正确的输出结果，保持外部信息（如数据库或文件）的完

整性。

③ 检测程序初始化和终止方面的错误。

2）白盒测试。白盒测试与黑盒测试不同，渗透测试工程师可以通过正常渠道向被测者要求取得各种资料，包括网络拓扑、员工资料甚至网站或其他程序的代码片断，也能够与被测组织内的其他员工（销售、程序员、管理者……）进行面对面的沟通。这类测试的目的是模拟客户组织内部雇员的越权操作，并预防万一组织重要信息泄露，网络黑客能利用这些信息对组织构成的危害。

测试目标不同，采用的技术也会有一定差异。测试者在系统网络的不同位置、不同攻击路径下进行渗透测试，结果反应的问题迥然不同。

3）内网测试。内网测试指的是渗透测试工程师由内部网络发起测试，这类测试能够模拟客户组织内部违规操作者的行为。

4）外网测试。外网测试指的是渗透测试工程师完全处于外部网络（如拨号、ADSL 或外部光纤），模拟从客户组织外部发起的攻击行为，可能来自于对客户组织内部信息一无所知的攻击者也可能来自于对客户组织内部信息一清二楚的攻击者。

（2）渗透测试流程 渗透测试可以分为 3 个阶段，分别为预攻击、攻击、后攻击，如图 20-1 所示。

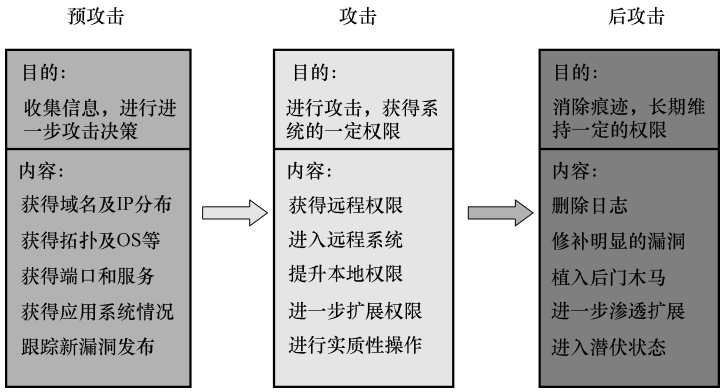


图 20-1 渗透过程图

1）预攻击阶段。

① 基本网络信息获取：

◇ ping 目标网络得到 IP 地址和 TTL 等信息。

◇ tcptraceroute 和 traceroute 的结果。

◇ whois 结果。

◇ netcraft 获取目标可能存在的域名、WEB 及服务器信息。

◇ curl 获取目标 WEB 基本信息。

◇ nmap 对网站进行端口扫描并判断操作系统类型。

◇ google、yahoo、baidu 等搜索引擎获取目标信息。

◇ 采用 FWtester、hping3 等工具进行防火墙规则探测。

② 常规漏洞扫描和采用商用软件进行检测：

◇ 结合使用游刃与 Nessus 等商用或免费的扫描工具进行漏洞扫描。

◇ 采用 SolarWind 对网络设备等进行发现。

◇ 采用 nikto、webinspect 等软件对 WEB 常见漏洞进行扫描。

◇ 采用如 AppDetective 之类的商用软件对数据库进行扫描分析。

③ 采用 WebProxy、SPIKEProxy、WebScarab、ParosProxy、Absinthe 等工具进行分析：

◇ 用 Ethereal 抓包协助分析。

◇ 用 webscan、fuzzer 进行 SQL 注入和 XSS 漏洞初步分析。

◇ 手工检测 SQL 注入和 XSS 漏洞。

◇ 采用类似 OScanner 的工具对数据库进行分析。

④ 应用分析的注意事项：

◇ 检查应用系统架构、防止用户绕过系统直接修改数据库。

◇ 检查身份认证模块，防止非法用户绕过身份认证。

◇ 检查数据库接口模块，防止用户获取系统权限。

◇ 检查文件接口模块，防止用户获取系统文件。

◇ 检查其他安全威胁。

2）攻击阶段。

① 基于通用设备、数据库、操作系统和应用的攻击。可以采用各种公开及私有的缓冲区溢出程序代码，一个比较好的 Exploit 搜索站点是：http：//www. frsirt. com/exploits/。也可以采用诸如 Metasploit Framework 之类的利用程序集合。

② 基于应用的攻击。基于 WEB、数据库或特定的 B/S 或 C/S 结构的网络应用程序存在的弱点进攻击，常见的如 SQL 注入攻击、跨站脚本攻击等，均属于这一类型。

③ 口令猜解技术。口令是信息安全里永恒的主题，进行口令猜解可以采用游刃、X-Scan、Brutus、Hydra、溯雪等工具。

3）后攻击阶段。

① 口令嗅探与键盘记录。通过嗅探、键盘记录、木马等软件获取客户相关口令及键盘信息。

② 口令破解。利用 L0phtCrack、JohntheRipper、Cain 等软件破解客户加密后的口令。

20.2 案例分析：银行渗透测试方案

某股份银行决定进行渗透测试，制定的渗透测试方案如下。

20.2.1 渗透目标和范围

1. 测试目标

1）更好地发现当前系统可能存在安全隐患，避免发生危害性的安全事件。

2）更好地为今后系统建设提供指导和有价值的意见及建议。

2. 测试的范围

本期渗透测试服务范围所包含的各个系统，可分为以下3类。

1）网站及WEB系统：门户网站、网银系统（含网站、对公对私客户端等）、信用卡网站（含网上商城、积分系统等）、企业年金WEB、机票代支付系统WEB、特结系统、二套MAIL系统。

2）WAP网站：手机银行。

3）专用设备：VPN远程管理系统专用设备、网络POS专用设备。

20.2.2 测试内容

1. 网站及WEB系统

针对网站及WEB系统的渗透测试，将进行以下方面的测试：

1）WEB服务器安全漏洞。

2）WEB服务器错误配置。

3）SQL注入。

4）XSS（跨站脚本）。

5）CRLF注入。

6）目录遍历。

7）文件包含。

8）输入验证。

9）认证。

10）逻辑错误。

11）Google Hacking。

12）密码保护区域猜测。

13）字典攻击。

14）特定的错误页面检测。

15）脆弱权限的目录。

16）危险的HTTP方法（如PUT、DELETE）。

2. WAP网站系统

针对WAP网站系统的渗透测试，将进行以下方面的测试：

1）WEB 服务器安全漏洞。
2）WEB 服务器错误配置。
3）SQL 注入。
4）XSS（跨站脚本）。
5）CRLF 注入。
6）目录遍历。
7）输入验证。
8）认证。
9）逻辑错误。
10）字典攻击。
11）特定的错误页面检测。

3. 专用设备

针对专用设备的渗透测试，将进行以下方面的测试（根据实际情况决定）：
1）SQL 注入。
2）XSS（跨站脚本）。
3）目录遍历。
4）输入验证。
5）认证。
6）逻辑错误。
7）字典攻击。
8）特定的错误页面检测。
9）脆弱权限的目录。

20.2.3 测试流程

1. 方案制定部分

渗透测试团队 GS 公司获取客户的书面授权许可后，才进行渗透测试的实施。并且就实施范围、方法、时间、人员等具体的方案与客户进行交流，得到了客户的认同。

在测试实施之前，渗透测试团队 GS 公司会做到让客户对渗透测试过程和风险的知晓，使随后的正式测试流程都在客户的控制下。

2. 信息收集部分

信息收集：操作系统类型指纹收集、网络拓扑结构分析、端口扫描和目标系统提供的服务识别等，可以采用一些商业安全评估系统（如 Unisscanner、极光等）、检测工具（NESSUS、Nmap 等）进行收集。

3. 测试实施部分

在规避防火墙、入侵检测、防毒软件等安全产品监控的条件下进行操作系统可检测

到的漏洞测试与应用系统检测到的漏洞测试（如 WEB 应用），此阶段如果成功的话，可能获得普通权限。

渗透测试人员可能用到的测试手段有扫描分析、溢出测试、口令爆破、社会工程学、客户端攻击、中间人攻击等，用于测试人员顺利完成工程。在获取到普通权限后，尝试由普通权限提升为管理员权限，获得对系统的完全控制权。此过程将循环进行，直到测试完成，最后由渗透测试人员清除中间数据。

4. 分析报告输出

渗透测试人员根据测试的过程结果编写直观的渗透测试服务报告。内容包括具体的操作步骤描述、响应分析及最后的安全修复建议。

20.2.4 测试工具

拟选用的测试工具如下：

1）拓扑分析工具：DNSSweep、Nslookup 等。

2）自动化扫描工具：极光、Unisscanner、Nessus、Retina、ISS、SSS 等。

3）端口扫描、服务检测：Nmap、SuperScan、THC-Amap 等。

4）密码、口令破解：Johntheripper、L0phtcrack、MD5Crack、Cain 等。

5）嗅探分析工具：Ethereal、Entercap、Dsniff 等。

6）拒绝服务（DoS）工具：HPING 等。

7）Exploiting 利用工具：Metasploit Framework、CoreImpact、Canvas 等。

8）应用缺陷分析工具：HDSI3、Domain3.5、sqlaccess 等。

20.2.5 测试的风险规避

在渗透测试过程中，尽量避免做影响正常业务运行的操作。但是由于测试过程变化多端，渗透测试服务仍然有可能对网络、系统运行造成不同程度的影响，严重的后果是可能造成服务停止，甚至是宕机。比如渗透人员实施系统权限提升操作时，突遇系统停电，再次重启时可能会出现系统无法启动的故障等。为此，拟采取以下多条策略来规避渗透测试带来的风险。

1. 备份策略

为防范渗透过程中的异常问题，测试的目标系统需要事先做一个完整的数据备份，以便在问题发生后能及时恢复工作。

对银行转账、电信计费、电力调度等不可接受可能风险的系统的测试，可以采取对目标副本进行渗透的方式加以实施。这样就需要完整的复制目标系统的环境，如硬件平台、操作系统、应用服务、程序软件、业务访问等，然后对该副本再进行渗透测试。

2. 应急策略

测试过程中，如果目标系统出现无响应、中断或者崩溃等情况，会立即中止渗透测

试，并配合客户技术人员进行修复处理等。在确认问题、修复系统、防范此故障再重演后，经客户方同意才能继续进行其余的测试。

3. 时间策略

为减轻渗透测试造成的压力和预备风险排除时间，安排测试的时间一般在业务量不高的时间段，比如夜间某个时间。

4. 测试策略

为了防范测试导致的业务中断，可以不做一些拒绝服务类的测试。非常重要的系统不建议做深入的测试，避免意外崩溃而造成不可挽回的损失；具体测试过程中，最终结果可以由测试人员做推测，而不实施危险的操作步骤加以验证等。

5. 沟通策略

测试过程中，确定测试人员和客户方配合人员的联系方式，便于及时沟通并解决工程中的难点。

第 21 章
安全运营技术

银行经过多年的安全建设，已经形成了覆盖多方面领域的安全专业系统，但是随着安全风险的日益变化，这些安全专业系统也带来了新的安全需求。

1）存在大量的边界网络安全设备（防火墙、IDS、IPS）、安全设备日志不统一、查看和归档烦琐，网络系统庞大并且持续增长，设备接入和维护工作日益繁重。

2）安全工作覆盖范围广，业务系统较多，资产无法迅速定位。

3）安全设备诸如防火墙、交换机、路由器等，存在日志不统一、查看和归档烦琐等问题。

4）安全告警多而复杂。在繁多的安全告警中，如何保证不会错过严重的、影响业务的告警，以及如何快速实时地响应处理。

5）事件分析关联性差，效率不高，分析报告可读性不高。

6）日常漏洞检查工作、基线加固工作繁重，严重影响工作效率和工作时间。

因此，对于银行来说，应建立主动安全的观念，建设一个安全集中的运营平台，实现对风险的集中管理，并部分解决以上安全管理和工作难题。同时，借助系统的建设，使得安全运维工作及人员得到有效监管，高效规范地对事件进行处理，对网络安全状况进行总体量化管理，很好地保障业务系统连续性。

21.1 系统安全运营技术

21.1.1 深度包检测技术（DPI）

深度包检测技术（DPI）是一种基于应用层的流量检测和控制技术，当 IP 数据包、TCP 或 UDP 数据流通过基于 DPI 技术的带宽管理系统时，该系统通过深入读取 IP 包载荷的内容来对 OSI 七层协议中的应用层信息进行重组，从而得到整个应用程序的内容，

然后按照系统定义的管理策略对流量进行整形操作。其检测技术有以下3种。

1. 基于“特征字”的识别技术

不同的应用通常依赖于不同的协议，而不同的协议都有其特殊的指纹，这些指纹可能是特定的端口、特定的字符串或者特定的比特序列。基于“特征字”的识别技术通过对业务流中特定数据报文中的“指纹”信息的检测，以确定业务流承载的应用。

根据具体检测方式的不同，基于“特征字”的识别技术又可以被分为固定位置特征字匹配、变动位置的特征匹配及状态特征匹配3种技术。通过对“指纹”信息的升级，基于“特征字”的识别技术可以很方便地进行功能扩展，实现对新协议的检测。如Bittorrent协议的识别，通过反向工程的方法对其对等协议进行分析，所谓对等协议指的是peer与peer之间交换信息的协议。对等协议由一个握手开始，后面是循环的消息流，每个消息的前面，都有一个数字来表示消息的长度。在其握手过程中，首先是先发送19，跟着是字符串“BitTorrent protocol”，那么“19BitTorrent Protocol”就是Bittorrent的“特征字”。

2. 应用层网关识别技术

某些业务的控制流和业务流是分离的，业务流没有任何特征。这种情况下，就需要采用应用层网关识别技术。应用层网关需要先识别出控制流，并根据控制流的协议通过特定的应用层网关对其进行解析，从协议内容中识别出相应的业务流。

对于每一个协议，需要有不同的应用层网关对其进行分析，如SIP、H323协议都属于这种类型。SIP/H323通过信令交互过程，协商得到其数据通道，一般是RTP格式封装的语音流。也就是说，纯粹检测RTP流并不能得出这条RTP流是通过哪种协议建立的。只有通过检测SIP/H323的协议交互，才能得到其完整的分析。

3. 行为模式识别技术

行为模式识别技术是基于对终端已经实施的行为的分析，判断出用户正在进行的动作或者即将实施的动作。行为模式识别技术通常用于无法根据协议判断的业务的识别。例如，SPAM（垃圾邮件）业务流和普通的E-Mail业务流从E-Mail的内容上看是完全一致的，只有通过对用户行为的分析，才能够准确的识别出SPAM业务。

以上3种识别技术分别用于不同类型协议的识别，无法相互替代。

深度包检测技术对网络流量的监控与检测，成为集中运营基础数据的重要来源之一。

21.1.2 大数据技术

2012年，“大数据”（Big Data）迅速成为全球信息技术界的热点，《纽约时报》表示“大数据时代已经降临”。大数据并非新概念，但2012年以来所提到的大数据包含了特定含义，必须具备以下4个特征，即Volume（体量），数据的规模庞大、增长速度快，从TB（1000GB）级别，跃升到PB（1000TB）甚至EB（1000PB）、ZB（1000EB）

级别；Variety（多样），数据的类型繁多、构成复杂，除了传统的结构化数据外，还包括了文字、语音、视频、文档、图片等多种非结构化数据；Value（价值），数据的价值潜力巨大，但隐藏较深，需要用综合多种复杂的分析算法对数据进行“提纯”；Velocity（速度），数据的处理速度快、时效性强，要进行实时或准实时的处理，并实时反馈处理结果。

总体来说，现代大数据的主体是非结构化数据。在当前的数据构成上，80% 的数据是非结构化或半结构化的，结构化数据仅有 20%。如果说对于结构化数据的处理和分析已经较为成熟的话，那么，对于非结构化数据的处理和分析才刚刚起步，但已经呈现出一派生机勃勃的景象，这也正是“大数据时代已经降临”的标志。

中国有着庞大的人群和应用市场，复杂且充满变化，如此庞大的用户群体，使中国即将成为世界上最大数据的国家，探索以大数据为基础的解决方案，是中国的银行提高自身竞争力的重要手段。可以说，大数据时代对银行的数据驾驭能力提出了新的挑战，也为银行获得更为深刻、全面的洞察能力提供了前所未有的空间与潜力。

大数据技术在集中运营中有广泛应用，是进行安全态势分析的重要技术。

21.1.3 数据融合技术

提到大数据，就必须提到数据融合（Data Fusion）。数据融合是指将来自多个信息源的数据收集起来，进行关联、组合，以提升数据的有效性和精确度。可以看出，数据融合的研究是大数据分析的基础性工作。目前，大部分安全态势分析的模型都是基于美国的军事机构 JDL 给出的数据融合模型衍生出来的（图 21-1）。

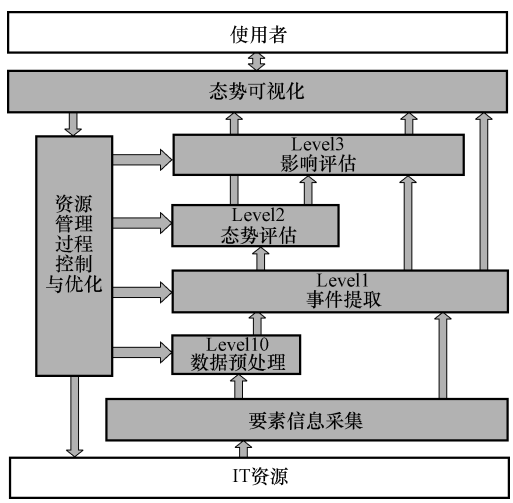


图 21-1　典型的态势感知模型

在这个基于人机交互的模型中，态势分析的实现被分为了 5 个级别（阶段），首先是对信息技术资源进行要素信息采集，然后经过不同级别的处理及其不断反馈，最终通过态势可视化实现人机交互。

（1）数据预处理　可选的级别，对于部分不够规整的数据进行预处理，如用户分布式处理、杂质过滤等。

（2）事件提取　是指要素信息采集后的事件标准化、修订，以及事件基本特征的扩展。

（3）态势评估　包括关联分析和态势分析。态势评估的结果是形成态势分析报告和网络综合态势图，为网络管理员提供辅助决策信息。

（4）影响评估　它将当前态势映射到未来，对参与者设想或预测行为的影响进行

评估。

（5）资源管理、过程控制与优化 通过建立一定的优化指标，对整个融合过程进行实时监控与评价，实现相关资源的最优分配。

由于网络空间态势分析的数据来自众多的网络设备，其数据格式、数据内容、数据质量千差万别，存储形式各异，表达的语义也不尽相同。如果能够将这些使用不同途径、来源于不同网络位置、具有不同格式的数据进行预处理，并在此基础上进行归一化融合操作，就可以为网络安全态势的感知提供更为全面、精准的数据源，从而得到更为准确的网络安全态势。

数据融合技术是一个多级、多层面的数据处理过程，主要完成对来自网络中具有相似或不同特征模式的多源信息进行互补集成，完成对数据的自动监测、关联、相关、估计及组合等处理，从而得到更为准确、可靠的结论。数据融合按信息抽象程度可分为从低到高的3个层次：数据级融合、特征级融合和决策级融合，其中特征级融合和决策级融合在态势分析中具有较为广泛的应用。

21.1.4 数据挖掘技术

安全集中运营采集大量网络设备和安全设备的数据，经过数据融合处理后，转化为格式统一的数据单元。这些数据单元数量庞大，携带的信息众多，有用信息与无用信息鱼龙混杂，难以辨识。要掌握相对准确、实时的网络安全态势，必须剔除干扰信息。数据挖掘就是指从大量的数据中挖掘出有用的信息，即从大量的、不完全的、有噪声的、模糊的、随机的实际应用数据中发现隐含的、规律的、事先未知的，但又有潜在用处的并且最终可理解的信息和知识的非平凡过程（Nontrivial Process）。

数据挖掘可分为描述性挖掘和预测性掘。描述性挖掘用于刻画数据库中数据的一般特性；预测性挖掘是在当前数据上进行推断，并加以预测。数据挖掘方法主要有关联分析法、序列模式分析法、分类分析法和聚类分析法。关联分析法用于挖掘数据之间的联系；序列模式分析法侧重于分析数据间的因果关系；分类分析法通过对预先定义好的类别建立分析模型，对数据进行分类，常用的模型有决策树模型、贝叶斯分类模型、神经网络模型等；聚类分析不依赖预先定义好的类别，它的划分是未知的，常用的方法有模糊聚类法、动态聚类法、基于密度的方法等。

21.1.5 可视化技术

网络安全态势生成是依据大量数据的分析结果来显示当前状态和未来趋势，而通过传统的文本或简单图形表示，使得寻找有用且关键的信息非常困难。可视化技术是利用计算机图形学和图像处理技术，将数据转换成图形或图像在屏幕上显示出来，并进行交互处理的理论、方法和技术。它涉及计算机图形学、图像处理、计算机视觉、计算机辅助设计等多个领域。目前已有很多研究将可视化技术和可视化工具应用于态势感知领

域，在网络安全态势感知的每一个阶段都充分利用可视化方法，将网络安全态势合并为连贯的网络安全态势图，快速发现网络安全威胁，直观把握网络安全状况。

21.2 系统安全态势感知技术

安全态势感知就是综合各方面的安全因素，从整体上动态反映网络安全状况，并对安全的发展趋势进行预测和预警。安全态势感知在信息安全领域随着 APT 检测的需求而流行，但其本质并不是新概念，属于信息安全技术里面的攻击探测技术。

在信息安全的早期，由于综合性的攻击探测要求比较高，单一性的探测技术和设备如 IDS 设备、防病毒系统等，成为实际业务中应用的主流。随着计算机和通信技术的迅速发展，计算机网络的应用越来越广泛，其规模越来越庞大，多层面的网络安全威胁和安全风险也在不断增加，网络攻击构成的威胁和损失也越来越大，网络攻击行为向着分布化、规模化、复杂化等趋势发展，仅仅依靠防火墙、入侵检测、防病毒、访问控制等单一的网络安全防护技术，已不能满足网络安全的需求，迫切需要综合的技术，才有可能及时发现网络中的异常事件，掌握网络安全状况，降低网络安全风险，提高网络安全防护能力，安全态势感知就应运而生。

实际工作中，导致安全态势感知技术在银行开始使用有两个关键因素：一是不断常态化的 APT（高级持续威胁）攻击，已经实实在在地展现上述单一安全防护措施的无能为力，综合防护的安全态势感知已经成为切实的需求；二是长期导致综合感知难以应用的技术屏障是海量数据，随着大数据技术的综合发展，有了质的突破。海量存储、并行计算、高效查询等技术均已成熟，为大规模网络安全态势感知技术的突破创造条件。

当前的安全态势感知技术实质就是借大数据分析，对成千上万的网络日志等信息进行自动分析处理与深度挖掘，从而感知网络中的异常事件与整体安全态势。

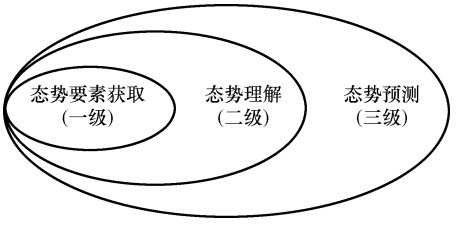


图 21-2 态势感知三级模型

态势感知的核心部分可以理解为一个渐进明晰的过程，其三级模型如图 21-2 所示。

态势感知首先是态势要素获取，抓取必要的数据；然后通过数据分析进行态势理解，进而实现对未来短期时间内的态势预测。态势感知的初步目标是态势的理解，为下一步决策提供支撑，最终目标是实现对未来的短期预测，为前瞻性的决策提供支撑。

安全态势感知的核心部分就是网络安全态势感知。而要感知网络安全态势，首先要感知网络态势。所谓网络态势是指由各种网络设备运行状态，以及在网络中传输数据等蕴含的网络行为或者用户行为等因素构成网络的当前状态和趋势变化。

网络态势感知（Cyberspace Situation Awareness，CSA）是 1999 年 Tim Bass 首次提出的，是在大规模的网络环境中，对能够引起网络态势发生变化的安全要素进行获取、

理解、显示，以及预测最近的发展趋势。

态势是一种状态、一种趋势，是整个和全局的概念，任何单一的情况或状态都不能称之为态势。因此对态势的理解特别强调环境性、动态性、整体性。环境性是指态势感知的应用环境是在一个较大的范围内具有一定规模的网络；动态性是态势随时间不断变化，态势信息不仅包括过去和当前的状态，还要对未来的趋势做出预测；整体行是态势各实体间相互关系的体现的状态，进而影响整个网络的态势。

网络安全态势感知就是利用数据融合、数据挖掘、智能分析和可视化等技术，直观显示网络环境的实时安全状况，为网络安全提供保障。借助网络安全态势感知，网络监管人员可以及时了解网络的状态、受攻击情况、攻击来源及哪些服务易受到攻击等情况；应急响应组织可以从网络安全态势中了解所服务网络的安全状况和发展趋势，为制定有预见性的应急预案提供基础。

网络安全态势感知的主要关注点有风险感知和事件感知两个方面。风险感知包括网络资产感知和网络脆弱性感知，网络资产感知是指自动、快速发现和收集大规模网络资产的分布情况、更新情况、属性等信息；网络脆弱性感知是分析、发现网络的脆弱性，对脆弱性进行统一标识和管理，网络脆弱性包括不可见脆弱性和可见脆弱性。事件感知主要包括安全事件感知和异常行为感知，安全事件感知是指能够确定安全事件发生的时间、地点、起因、经过和结果；异常行为感知是指通过异常行为判定风险，以弥补对不可见脆弱性、未知安全事件发现的不足，主要面向的是感知未知的攻击。

21.3 系统安全运营的内容与流程

21.3.1 安全运营的内容

安全运营的主要内容有以下几个方面：

1）数据采集。完成安全域内和域间的流量数据采集，以及相关网络设备、安全设备的日志采集。

2）数据处理和安全态势感知。

3）依托安全态势感知平台对采集的数据进行分析、挖掘，利用各种综合技术，实现对安全态势的感知与预测。

4）安全事件的监控和预警。

5）根据安全事件的管理要求，监控安全事件，并及时预警。

6）安全事件的响应与处理。

7）根据应急响应的要求和规范，相应安全事件，及时处置，事后分析总结，完整地处理安全事件。

21.3.2 安全运营流程

在安全运营过程中，基于“PDCA”循环理论，结合安全运营的四大内容，完整的安全运营管理体系，以实现安全风险事件的全生命周期管理，具体的安全运营流程，见图 21-3。

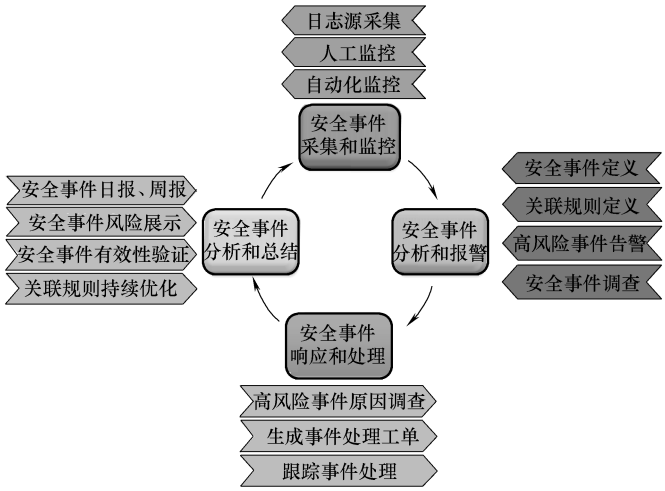


图 21-3 安全运营流程

第 22 章
灾难备份与恢复技术

灾难备份是为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、专业技术支持能力和运行管理能力进行备份的过程。

灾难恢复是为了将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态、并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态而设计的活动和流程。

衡量灾备系统的两个重要指标是：

1）恢复时间目标（Recovery Time Objective，RTO）：灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求。RTO 标志着系统能够容忍的服务停止的最长时间。系统服务的紧迫性要求越高，RTO 的值越小，灾备能力就越高。

2）恢复点目标（Recovery Point Objective，RPO）：灾难发生后，系统和数据必须恢复到的时间点要求。RPO 标志着系统能够容忍的最大数据丢失量。系统容忍丢失的数据量越小，RPO 的值越小。若 RPO 等于 0，相当于没有任何数据丢失。否则，就需要进行业务回复处理，对丢失数据进行修复。

RPO 针对的是数据丢失，RTO 针对的是服务丢失，两者必须在进行风险分析和业务影响分析之后根据业务的需求来确定（表 22-1）。

表 22-1　灾备等级要求与灾备技术表

灾备等级	RTO	RPO	可用技术
1	2 天以上	1 ~ 7 天	基于磁带的备份
2	24 小时以后	1 ~ 7 天	基于磁带的备份
3	12 小时以上	数小时至 1 天	基于磁带的备份（或虚拟带库）
4	数小时至 2 天	数小时至 1 天	基于存储复制、存储交换层复制或主机软件复制/异步镜像
5	数分至 2 天	0 ~ 30 分钟	基于存储复制、存储交换层复制或同步镜像
6	数分钟	0	同步镜像 + 集群技术

22.1 技术与发展趋势

一般来讲，灾备系统可以分为数据级容灾、应用级容灾和业务级容灾。

1）数据级容灾是指通过建立异地容灾中心，做数据的远程备份，在灾难发生之后要确保原有的数据不会丢失或者遭到破坏；但在数据级容灾这个级别，发生灾难时应用是会中断的。在数据级容灾方式下，所建立的异地容灾中心可以简单地理解成一个远程的数据备份中心。数据级容灾的恢复时间比较长，但是相比其他容灾级别来讲，它的费用比较低，而且构建实施也相对简单。

2）应用级容灾是在数据级容灾的基础之上，在备份站点同样构建一套相同的应用系统，通过同步或异步复制技术，这样可以保证关键应用在允许的时间范围内恢复运行，尽可能减少灾难带来的损失，让用户基本感受不到灾难的发生，这样就使系统所提供的服务是完整的、可靠的和安全的。应用级容灾生产中心和异地灾备中心之间的数据传输是采用异类的广域网传输方式；同时，应用级容灾系统需要通过更多的软件来实现，可以使多种应用在灾难发生时进行快速切换，确保业务的连续性。

3）业务级容灾是全业务的灾备，除了必要的信息技术相关技术，还要求具备全部的基础设施。其大部分内容是非信息技术系统（如电话、办公地点等），当大灾难发生后，原有的办公场所都会受到破坏，除了数据和应用的恢复，更需要一个备份的工作场所能够正常地开展业务。

下面主要针对数据级容灾进行介绍。

22.1.1 数据存储技术

数据存储备份就是把数据从生产系统备份到存储备份系统中的存储介质的过程。因此，存储优化是提高灾难备份系统性能的重要指标之一。目前，比较通用的技术有网络附加存储（Network Attached Storage，NAS）和存储区域网络（Storage Area Network，SAN）。

1）NAS 是将存储设备连接到现有的网络上，提供数据和文件服务。NAS 服务器一般由存储硬件、操作系统及其中的文件系统等几个部分组成。NAS 实现简单，建立方便，设备不依赖于操作系统，数据的存储和处理功能分离，价格较低。

2）SAN 是通过特定的互联方式连接的若干台存储服务器组成一个单独的数据网络。SAN 的硬件基础设施是光纤通道，由 3 部分构成：存储和备份设备（包括磁盘阵列和磁带库等）、光纤通道网络连接部件（包括交换机、HBA 卡、光缆线、集线器、光纤通道与 SCSI 间的桥接器等）和应用管理软件（包括备份软件、存储资源管理软件、设备管理软件等）。SAN 是一种特殊的高速网络，连接网络服务器和诸如大磁盘阵列或备份磁带库的存储设备，SAN 不依赖于 LAN，允许任何服务器连接到任何存储阵列，

可以提供大容量的存储数据服务。与 NAS 相比，SAN 的成本较高。

22.1.2 数据复制技术

数据复制技术即数据镜像技术。与数据存储技术相比，数据复制技术则是通过不断将生产系统的数据复制到另外一个不同的备份系统中，以保证在灾难发生时，生产系统的数据丢失量最少。

下面主要针对基于传统备份、数据库复制、存储复制、存储交换层复制、主机软件复制技术进行详细介绍。除了基于数据库的数据复制外，其他技术都具有同步和异步两种复制方式。同步数据复制就是将本地生产系统的数据以完全同步的方式复制到备份系统中。由于发生在生产系统的每一次 I/O 操作都需要等待远程复制完成才能返回，这种复制方式虽然可能做到数据的零丢失，但是对系统性能有很大的影响。异步数据复制则是将本地生产系统中的数据在后台以异步的方式复制到备份系统中。这种复制方式会有少量的数据丢失，但是对生产系统的性能影响较小。在灾备中心的建设过程中，应根据应用需求和数据复制技术的优缺点选择不同的灾难备份策略。

1. 传统备份的灾备技术

下面以磁带备份灾备方案为例，介绍传统备份的灾备技术（图 22-1）。

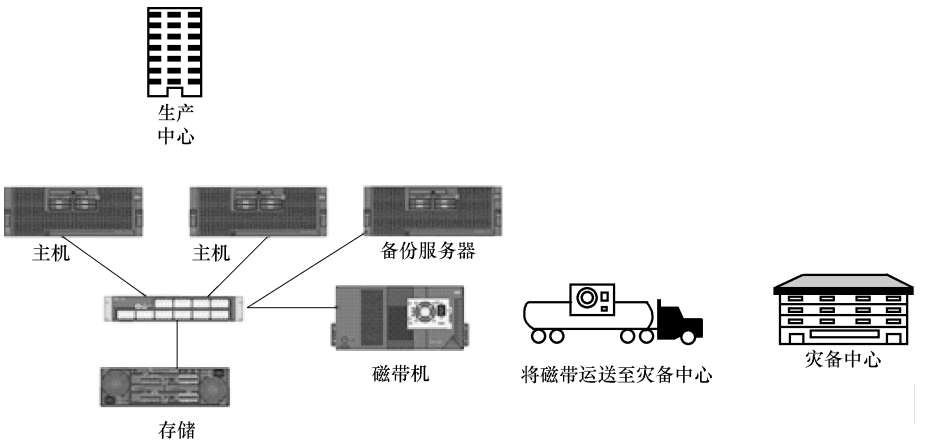


图 22-1 磁带备份灾备方案

（1）方案简述 利用传统备份技术，在生产中心搭建本地备份系统，通过备份服务器，设定备份策略，依据备份策略，可对所需保护数据进行全备、增量备份及合成备份等，灾备建设通常将数据备份两份，一份本地保存，另一份运送至灾备中心，当发生灾难时，可通过灾备中心数据进行数据恢复。

（2）增加设备及软件 备份服务器、磁带机、备份软件。

（3）方案优势 传统备份技术的实现已经被当前的用户大量应用并被熟知，传统备份技术的成熟度及成本上具备的优势，可支持各种平台及数据库，支持复杂环境，可通过 LAN 或 SAN 网络进行数据备份。

（4）方案缺点

1）备份时间长，无法实现实时灾备。

2）灾备数据的有效性检测复杂，且数据格式在备份过程中进行了转换，恢复时间长。

3）需要安排人员运送磁带至灾备中心。

近几年，传统备份技术有了一定的优化，出现了磁盘到磁盘（D2D）、磁盘到磁盘再备份至磁带（D2D2T）及虚拟带库等技术，这几类技术的出现大大缩短了备份窗口时间，但总体上与其他灾备技术相比，灾备的实时性、恢复可靠性和恢复时间相对处于劣势。

2. 基于数据库复制技术（图 22-2）

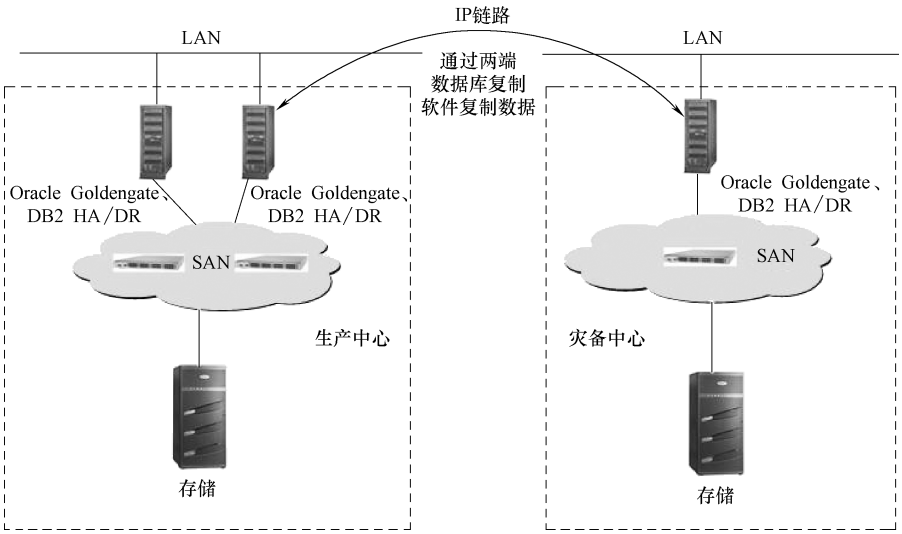


图 22-2　数据库复制示意图

（1）方案简述　此类方案是针对数据库应用的灾备实现，数据同步模式是基于事务处理级别。在生产中心数据库服务器及灾备中心数据库服务器安装对应的数据库复制软件后，生产中心数据库的每个事务处理操作，都会在灾备中心数据库系统中重复执行，也就是通常大家所说的 SQL 写操作日志的重复。数据库复制软件通过解析源数据库在线日志或归档日志获得数据的增删改变化，将这些变化应用到目标数据库，实现源数据库与目标数据库同步、双活。生产中心与灾备中心的数据复制链路采用 IP 或专线进行数据传输。

（2）增加设备

1）生产中心：为服务器安装数据库复制软件，配置与灾备中心的 IP 或专线连接。

2）灾备中心：配置与生产中心相同的操作系统及满足处理能力要求的服务器，并安装数据库复制软件，配置满足存储能力要求的磁盘阵列设备。

（3）方案优点

1）IP 网作为复制链路，成本低。

2）支持异构存储。

3）可保证两端数据库的事务一致性。

（4）方案缺点

1）复制软件需要生产中心及灾备中心的数据库版本必须一致，软件扩展的难度高、维护和恢复难度高，实施工作量也相对较高，需要由精通数据库的专业人员实施及运维。

2）无法实现数据库数据统一复制，需要为每一类数据库配置对应的数据库复制软件。

3）数据库灾备只能保护数据库数据，无法保护其他数据类型。

4）第三方工具需要单独购买，成本较高。

3. 基于主机软件复制技术（图 22-3）

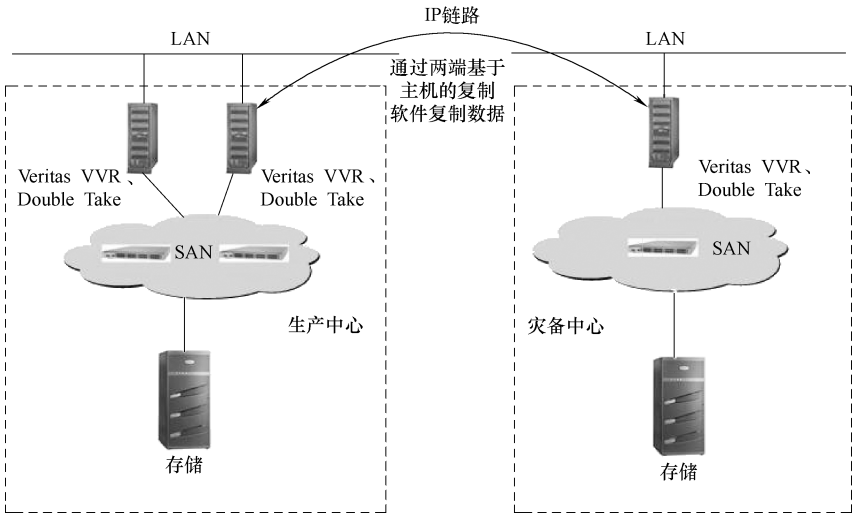


图 22-3　主机软件复制示意图

（1）方案简述　为生产中心及灾备中心服务器安装复制软件，配置复制策略，通过 TCP/IP 或专线网络链路，生产中心主机实时复制所需保护卷或者文件至灾备中心主机。生产中心与灾备中心的数据复制链路采用 IP 或专线进行数据传输。

（2）新增设备

1）生产中心：服务器安装主机复制软件，配置与灾备中心的 IP 或专线连接。

2）灾备中心：配置与生产中心相同的操作系统及满足处理能力要求的服务器，并安装主机复制软件，配置满足存储能力要求的磁盘阵列设备。

（3）方案优点

1）独立于硬件的支持，无硬件兼容性层面的局限性。

2）字节级或数据块级同步或异步的数据复制，只复制数据的变化量，IP 网作为复制链路，支持异构存储。

3）复制模式较灵活，可复制数据库数据及文件数据。

4）扩展性强，满足新功能、新业务的增加在原有的系统平台上扩展和实现。

（4）方案缺点

1）在正常情况下，占用一部分 CPU 及其他服务器的资源。

2）对现有系统改动较大。生产中心业务数据需进行数据迁移及备份，生产中心应用系统需改造成为 Veritas 文件系统，灾备中心应用系统也要配置成为 Veritas 文件系统，才能使用 VVR（VERITAS Volume Replicator）进行远程容灾；生产中心的业务数据还需迁移回去。因此实施工作量相对较大，实施难度相对较高。

3）在服务器数量较多的环境下，管理程度复杂，整体投入成本较大。

4）只适用于新建生产中心的业务系统。

4. 基于存储交换层复制技术（图 22-4）

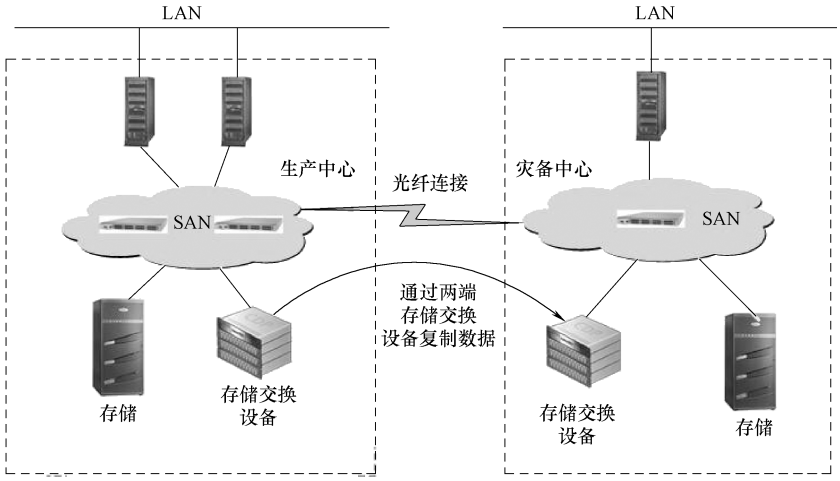


图 22-4　存储交换层复制示意图

（1）方案简述　生产中心及灾备中心各新增一套存储交换设备至 SAN 存储网络，生产中心存储交换设备将捕捉经过 SAN 交换机的数据，复制至灾备中心存储交换设备。

此类技术主要是基于存储网络的虚拟化技术实现灾备，能打破灾备建设中存储阵列的类型和品牌限制，能进行多个存储阵列环境下的统一灾备。

利用生产中心和灾备中心存储交换设备的复制功能，就可以在灾备中心获得生产中心完整的各时间点数据，同时，生产中心拥有的任何恢复功能在异地的灾备中心同样具备。

生产中心与灾备中心的数据复制链路采用光纤或专线进行数据传输。

（2）新增设备

1）生产中心：新增一套存储交换设备，配置与灾备中心的光纤或专线连接。

2）灾备中心：新增一套存储交换设备。

（3）方案优点

1）支持异构存储，能进行多个存储设备的统一灾备，降低灾备运维复杂度。

2）数据一致性好。

3）可以防范逻辑灾难。

4）易于实施和维护。

（4）方案缺点 对生产系统性能有一定影响。

5. 基于存储复制技术（图 22-5）

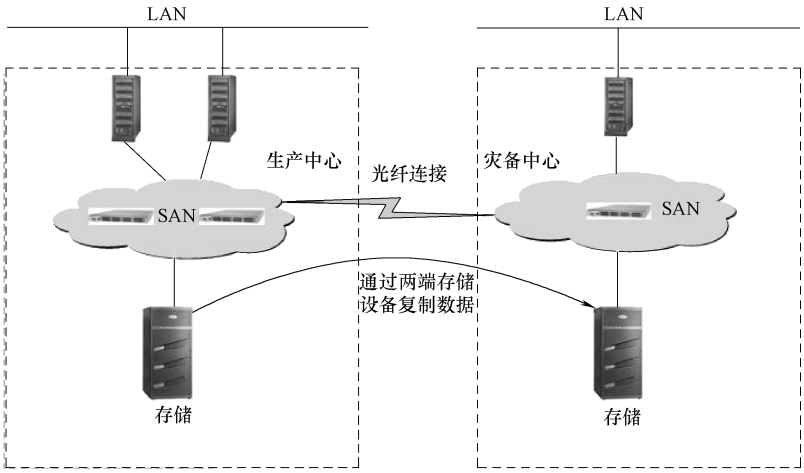


图 22-5 存储复制示意图

（1）方案简述 通过存储控制器实现的设备级数据远程镜像或复制，是传统灾备方式中最高效最可靠的方式。

基于存储复制技术的关键是实现盘阵之间的直接镜像，通过存储系统内建的固件（Firmware）或操作系统，利用 DWDM、光纤通道等传输界面连接，将数据以同步或异步的方式复制到远端。基于存储复制技术将数据与应用系统分开，对主机系统的运行资源影响比较小。另外，由于运行机制大多是利用镜像来复制数据，并借助高速缓冲存储器加速 I/O 存取，两端的数据差异时间点比较小，加上存储系统本身具备一定的容错能力，使之具有较高的运行性能和可靠性。

生产中心与灾备中心的数据复制链路采用光纤或专线进行数据传输。

（2）新增设备

1）生产中心：存储设备配置远程复制软件，配置与灾备中心的光纤或专线连接。

2）灾备中心：配置一套与生产中心相同的具备远程复制功能的存储设备。

（3）方案优势

1）对应用透明，可以实现所有应用的灾备，支持所有的数据类型，是最全面的灾备保护模式。

2）基于专有的硬件来进行数据同步，灾备的性能有保障，无须占用主机资源。

3）技术成熟，应用广泛，运行维护容易。

（4）方案缺点

1）需要对生产系统进行存储整合，涉及系统架构调整。

2）兼容性较差，不能跨越品牌，只能在相同的产品甚至是相同的型号之间实现

灾备。

3）设备成本投入相对较高，网络带宽要求较高。

6. 技术对比

以上介绍的4种复制技术的对比列表，见表22-2。

表22-2　技术对比列表

复制技术 / 影响因素	基于数据库复制技术	基于主机软件复制技术	基于存储交换层复制技术	基于存储复制技术
总体投资规模	中低	中	中低	高
理想距离	<1000km	<100km(同步) <1000km(异步)	无距离限制	<100km(异步) 无带宽距离限制
数据集中存储要求	不要求	不要求	要求	要求
实施难度	中	中	低	中
适应范围和约束条件	网络带宽要求较低 简单应用环境	高网络带宽 特定的文件系统格式	网络带宽要求一般	专用存储连接链路 高端存储设备
技术成熟度	一般	成熟	成熟	成熟
对系统性能的影响	中	中	中	小
运行维护的要求	较高	中	小	低
RPO	通常异步,分钟级	同步:0 异步:分钟级	同步:0 异步:分钟级	同步:0 异步:分钟级

22.1.3　技术发展趋势

在当前情况下，技术也呈现不断发展的态势，体现在以下几方面。

1. 存储虚拟化（Storage Virtualization）技术

通过虚拟化技术，用户可以利用已有的硬件资源，把SAN内部的各种异构的存储资源统一成对用户来说是单一视图的存储池（Storage Pool），方便用户可以根据自己的需求对这个大的存储池进行分割、分配。另外也可以根据业务的需要，实现存储池对服务器的动态而透明的增长与缩减。

通过存储虚拟化技术可实现数据的远程复制，以确保灾备中心与生产中心的数据保持同步以实现数据容灾。存储虚拟化技术可以在不同层面实现，如智能交换机层面、存储层面或增加第三方设备层面。采用虚拟存储技术进行数据复制同样也可以有同步复制方案和异步复制方案，需要根据具体的需求选择合适的产品。

2. 重复数据删除技术

该技术通过寻找不同数据块中的冗余数据并删除这些重复的数据来对数据进行压缩。某些重复数据压缩技术甚至实现了20:1的压缩比。通过重复数据删除技术不但能解决单

数据中心中多副本占用空间的问题，还可以减少传输备份数据所需要的带宽。重复数据删除技术主要分为基于软件的重复数据删除和基于硬件的重复数据删除两种方式。

3. 持续数据保护（CDP）技术

CDP 是一种在不影响主要数据运行的前提下，实现持续捕捉或跟踪目标数据所发生的任何变化，并且能够恢复到此前任意时间点的方法。CDP 系统能够提供块级、文件级和应用级的备份，以及恢复目标的无限的任意可变的恢复点。

22.2 灾难备份系统技术方案的实现

22.2.1 技术方案的设计

根据灾难恢复策略制定相应的灾难备份系统技术方案，包含数据备份系统、备用数据处理系统和备用的网络系统。技术方案中所设计的系统，应获得同主系统相当的安全保护，具有可扩展性，考虑其对主系统可用性和性能的影响。

22.2.2 技术方案的验证、确认和系统开发

为确保技术方案满足灾难恢复策略的要求，应由组织的相关部门对技术方案进行确认和验证，并记录和保存验证及确认的结果。按照确认的灾难备份系统技术方案进行开发，实现所要求的数据备份系统、备用数据处理系统和备用网络系统。

22.2.3 系统安装和测试

按照经过确认的技术方案，灾难恢复规划实施组应制订各阶段的系统安装及测试计划，以及支持不同关键业务功能的系统安装及测试计划，并组织最终用户共同进行测试。确认以下各项功能可正确实现：

1）数据备份及数据恢复功能。

2）在限定的时间内，利用备份数据正确恢复系统、应用软件及各类数据，并可正确恢复各项关键业务功能。

3）客户端可与备用数据处理系统正常通信功能。

22.3 灾难恢复策略的制定

数据备份策略（Data Backup Strategy）是为了达到数据恢复和重建目标所确定的备

份步骤和行为。通过确定备份时间、技术、介质和场外存放方式，以保证达到恢复时间目标和恢复点目标。

灾难恢复策略主要包括灾难恢复资源的获取方式、灾难恢复资源各要素的具体要求。

22.3.1 灾难恢复资源的获取方式

1. 数据备份系统

数据备份系统可由组织自行建设，也可通过租用其他机构的系统而获取。

2. 备用数据处理系统

可选用以下方式来获取备用数据处理系统：

1）事先与厂商签订紧急供货协议。

2）事先购买所需的数据处理设备并存放在灾难备份中心或安全的设备仓库。

3）利用商业化灾难备份中心或签有互惠协议的机构已有的兼容设备。

3. 备用网络系统

备用网络通信设备可通过上述的方式获取；备用数据通信线路可使用自有数据通信线路或租用公用数据通信线路。

4. 备用基础设施

可选用以下 3 种方式获取备用基础设施

1）由组织所有或运行。

2）多方共建或通过互惠协议获取。

3）租用商业化灾难备份中心的基础设施。

5. 专业技术支持能力

可选用以下几种方式获取专业技术支持能力：

1）灾难备份中心设置专职技术支持人员。

2）与厂商签订技术支持或服务合同。

3）由主中心技术支持人员兼任。

4）但对于 RTO 较短的关键业务功能，应考虑到灾难发生时交通和通信的不正常，造成技术支持人员无法提供有效支持的情况。

6. 运行维护管理能力

可选用以下对灾难备份中心的运行维护管理模式：

1）自行运行和维护。

2）委托其他机构运行和维护。

7. 灾难恢复预案

可选用以下方式完成灾难恢复预案的制订、落实和管理：

1）由组织独立完成。

2）聘请具有相应资质的外部专家指导完成。

3）委托具有相应资质的外部机构完成。

22.3.2 灾难恢复资源的要求

1. 数据备份系统

组织应根据灾难恢复目标，按照成本风险平衡原则，确定数据备份的范围、数据备份的时间间隔、数据备份的技术及介质、数据备份线路的速率及相关通信设备的规格和要求。

2. 备用数据处理系统

组织应根据关键业务功能的灾难恢复对备用数据处理系统的要求和未来发展的需要，按照成本风险平衡原则，确定备用数据处理系统的数据处理能力、与主系统的兼容性要求、平时处于就绪还是运行状态。

3. 备用网络系统

组织应根据关键业务功能的灾难恢复对网络容量及切换时间的要求和未来发展的需要，按照成本风险平衡原则，选择备用数据通信的技术和线路带宽，确定网络通信设备的功能和容量，保证灾难恢复时，最终用户能以一定速率连接到备用数据处理系统。

4. 备用基础设施

组织应根据灾难恢复目标，按照成本风险平衡原则，确定对备用基础设施的要求，包括与主中心的距离要求、场地和环境（如面积、温度、湿度、防火、电力和工作时间等）要求、运行维护和管理要求。

5. 专业技术支持能力

组织应根据灾难恢复目标，按照成本风险平衡原则，确定灾难备份中心在软件、硬件和网络等方面的技术支持要求，包括技术支持的组织架构、各类技术支持人员的数量和素质等要求。

6. 运行维护管理能力

组织应根据灾难恢复目标，按照成本风险平衡原则，确定灾难备份中心运行维护管理要求，包括运行维护管理组织架构、人员的数量和素质、运行维护管理制度等要求。

7. 灾难恢复预案

组织应根据需求分析的结果，按照成本风险平衡原则，明确灾难恢复预案的整体要求，制订过程的要求，教育、培训和演练要求，以及管理要求。

第四篇

实践篇

第 23 章
银行信息安全风险管理实践与案例

23.1 某股份制商业银行安保平台建设实例

23.1.1 安保平台建设背景

随着我国金融环境和信息化技术应用的快速发展，国内银行综合业务系统的发展由手工操作的电算化登记簿概念的单机版时代，快速步入了以数据集中、面向交易为特点的综合业务系统时代。在银行新综合业务系统进入数据大集中阶段后，各家银行更加强调以客户为中心，在行内统一客户视图，满足客户个性化的金融服务需求。为此，某股份制商业银行（以下简称 C 行）在其新综合业务系统就采用了一套全新的思路、理念和技术路线，构建切合 C 行实际发展需要的“流程银行”支撑系统，实现了业务流程再造和业务与技术模块化实施等突出特点。

作为 C 行新综合业务系统的业务和技术架构中的重要支撑模块之一，安全服务保障平台系统（简称安保平台）应运而生，其主要功能是为新综合业务系统的所有应用模块提供综合密码安全服务和用户认证管理功能。与新综合业务系统一样，这是一个以新的思路和理念构建的安全功能模块。C 行历来重视信息安全工作，受历史原因和技术条件的限制，某些应用系统在建设之初，其用户、密码的安全管理几乎都是各自为政的局面，难以站在一个全局的角度规划密码应用安全的方方面面。造成现有信息系统中的密码应用安全等级和强度参差不齐，难以统一对用户认证与权限进行管理，特别是某些安全设备当中的敏感密钥信息还做不到高效和便捷的更新，存在一定的安全隐患和脆弱点，并对整个应用系统的安全运行管理造成极大的不便。

在这样的建设背景和实现情况下，C 行谋求在密码和用户认证应用安全上，建立一个统一的安全服务保障平台，其建设需求及实现目标如下：

1）从C行信息科技的全局视角和高度出发，通盘考虑用户认证及密码应用安全风险，将各种业务应用系统的安全等级和强度提到相同的高度，以满足业务应用和安全审计的需要。即通过建立统一的安全服务平台，强化和规范应用系统秘钥管理及用户认证安全措施，向各种应用提供全面的安全服务调用机制，实现多渠道、多认证方式的应用安全服务保障体系。

2）将C行所采用的各种用户安全机制进行分析、整理和归类。这些机制包括鉴别银行客户的卡、折必备的PIN/卡安全机制（PVV/CVV），通过银行和公安部鉴别客户身份的身份核查机制，处理银行常用票据所用到的印鉴验证、支付密码验证、汇票密押核验、一票一密鉴定等安全机制，用于银行柜员或员工身份鉴别的指纹、令牌（USBKey）、高强度密码等安全机制，用于银行与其他渠道或外联系统（人行、银联、证券、其他第三方机构、网银、电话银行）处理相关业务的应用密钥转换和管理安全机制，为保证应用安全处理敏感数据所用到数据加解密、防篡改、防抵赖的安全机制，为应用系统统一进行用户与权限管理的用户标识定义、权限定义、角色定义和分配机制等。上述这些安全机制，经过综合分析和集中处理后，以安全服务的形式构建在安保平台的安全服务模块中。同时，依据相关管理机构的标准和规范，并借鉴其他银行应用安全建设经验，构建多个类别的安全服务功能模块或接口，以可定制的标准服务方式为各种业务系统提供安全服务保障。

3）为满足银行应用安全架构整体设计的需要和行业安全标准及规范，应对平台所涉及的特殊安全设备进行定制开发，这些设备包括加密机设备、令牌设备、加密的密码输入键盘设备等。

4）安全服务平台应是为整个应用安全架构体系提供信任或认证支撑的基础设施平台。在银行的综合业务系统应用安全建设中，需要与这些基础设施的连接和相关应用接口的定制和开发。这些基础设施可以采用标准的PKI/CA技术，有特定的应用目标；也可以采用我国自主知识产权并得到国家相关管理部门批准的标识认证技术，如CPK认证技术。除了上述基础设施外，C行还要扩充多种认证手段，并使用多种认证协议，如LDAP/DB、REDIUS、Active Directory、短信OTP、TOKEN OTP、IC卡等。

5）除了上述因素外，为保证安全服务正常的服务功能，还需要对安全服务的关键要素进行有效的配置和管理。这些关键要素主要包括安全设备管理及相关密钥管理。在银行的现有系统中，安全设备及相关密钥的管理，还显得比较分散和凌乱，各应用业务系统之间的安全设备几乎没有什么关联关系，设备信息都是一些相对独立的信息孤岛，这就为安全设备的统一管理和维护造成极大的困难。现有应用系统的密钥存放和管理也相对零散，而密钥管理的安全强度也不相统一，有些应用密钥存储和交换的安全隐患还相当明显。为从系统结构上克服上述局限性，需构建统一的安全设备与密钥管理平台。在安全设备与密钥管理平台中，针对设备及密钥的生命周期，设计严格的管理流程和管理规范，从而实现对安全设备及密钥较为规范的管理和维护。整理管理环节做到了统一、安全、有效。

6）在银行应用安全建设中，除了业务应用系统可以使用统一、规范、强度适宜的

各种安全服务以保证业务处理的安全性外，还要对使用业务应用系统的具体使用者或操作用户、设备、程序等进行统一的编码标识、定义他们在业务处理中采用的鉴别方式及统一定义在业务处理过程中的处理权限，也就通常意义上所说的 ID 管理和权限管理。鉴于此，需要构建统一的 ID 管理平台和用户与权限管理平台，以完成上述使命。在这种机制下，各个业务应用系统的使用者或操作者的权限都是通过此用户与权限管理平台统一定义的。用户具体操作或使用时，通过调用安保平台的登录服务并获得相应的操作权限，业务应用系统对使用者的权限进行检查和控制。这样就保证了在应用系统的相关权限变更时，必须通过统一的用户与权限管理平台，而业务应用系统本身无法随意更改权限，从而实现权限的统一安全管理。

7）为了满足整个业务系统安全信息的合规性和可追溯性，需要建立统一的日志统一采集、分析平台。目的是收集所有应用系统包括安全服务保障平台本身的日志信息，统一存储，并为最终进行的安全分析和审计做好充足的证据和数据准备。

23.1.2 安保平台建设基本思路

1. 走平台化、体系化、系统化的建设路线

为强化安全服务及保障系统的整体性、可管理性等建设方面的重要性，安保平台应走平台化、体系化、系统化的建设路线。安保平台的体系化、系统化建设表现在，应站在整个企业的高度，围绕企业的业务目标及配套的信息资产风险管理机制，持续不断地对系统潜在的风险进行评估、加固、运维检查，并且在整个系统的生命周期内，循环进行，避免重复投入和重新建设。同时强调在循环过程中的安全功能、风险管理机制建设的系统化咨询及对业务员工的安全意识培养和教育。

2. 尊重科学规律，兼顾近期项目要求及系统长远建设需求

安保平台项目首先是一个典型的安全项目，其具体实施要遵循标准的安全项目实施阶段的定义，即了解系统安全保障要求、安全需求分析、系统安全架构设计、系统详细设计、系统实施，以及贯穿在上述几个阶段实时评估安全机制的有效性。其次，安保平台项目又是一个服务于新综合业务系统各个应用，乃至 C 行信息网络系统全局的支撑系统，项目任务整体建设繁重而复杂，任重而道远，特别需要兼顾近期项目要求及 C 行信息系统全局的长远建设要求，整体策划、分步实施。

3. 突出自主创新与企业特色

安保平台项目既要依托于传统的安全技术、软件、硬件技术，又要不吝于发挥自主创新意识，使用一些经过项目实践验证且尚未被广泛认知的技术、机制等，体现出 C 行勇于创新的企业特色。比如组合公钥密码技术——CPK 认证技术。

4. 强调安保平台建设的标准化、规范化及合规性

安保平台项目是个服务于金融或银行领域业务系统的基础支撑项目，在这个领域要遵循国内外及行业的安全技术及管理标准。同时，银行新综合业务系统是事关国计民生

的基础设施，银行的主管和监管机构也发布了众多的管理办法和指引，所以安保平台建设的合规性问题，也是要高度重视并要达到相应管理要求的。

5. 服务于业务应用系统，力争提供全面的密码安全产品线

在新综合业务系统的技术架构中，安保平台是服务于各种业务系统、应用系统的综合安全支撑平台。按照这样的设计思想，安保平台除了提供金融、交易类的安全产品外，还要提供即能面向银行员工又能面向银行客户的 ID 管理、身份及标识认证、授权权限管理和控制、安全审计与风险控制等全方位的安全产品线，以满足各种渠道、通道乃至后台系统、运维/运营应用系统的安全保障需要。

6. 立足于风险管理和控制

鉴于银行业对信息科技系统的风险管理与控制向来非常重视，作为重要支撑模块之一的安保平台，一方面对综合业务系统整体的风险管理与控制提供充足的支撑与保障，另一方面在自身的系统建设过程，也要考虑自身的风险管理与控制机制。

23.1.3 安保平台建设过程

1. 项目主要阶段划分

对应 C 行新综合业务系统项目建设目标，安保平台项目可分为以下几个阶段，而在每个阶段，安保平台也具有特定的工作重点。

1）安全保障需求了解及应用安全需求分析阶段。

2）基础功能设计开发及安全设备定制阶段。

3）系统功能升级阶段。

4）公私分拆后的系统调整、模拟演练及上线准备阶段。

5）基础设施扩充及完善阶段。

2. 项目各阶段的工作重点

1）安全保障需求了解及应用安全需求分析阶段。按照标准的安全项目实施模型（SE-CMM）的定义，首先是要完成挖掘应用系统敏感数据资产的保护要求，并进行核心银行系统乃至安保平台的安全需求具体分析。在此阶段，安保项目组成员对 C 行老系统中的几十个与安全密切的应用，包括已有的安全功能模块进行大规模的重新梳理工作。鉴于在项目的初始阶段，安保项目组的公司成员对银行的各种业务了解程度有限，因而在沟通与梳理工作方面花费了相当多的精力，也克服了许多困难，最终梳理出来了需要安保平台提供的并服务于应用系统的安全服务功能初步需求和安全服务管理初步需求。

2）基础功能设计开发及安全设备定制阶段。在此阶段，涉及 SE-CMM 模型的 3 个阶段，即安全架构设计、系统详细设计和项目实施阶段。基于前面的需求分析工作，并依据 C 行统一的流程、银行综合业务系统的业务架构及技术架构，一个适合于 C 行业务系统的安全技术架构应运而生。依据此架构，项目组完成针对安全基础功能的详细设

计和代码研发及相关的具体实施工作。在安全技术架构中，首先，应用系统及其用户是安保平台的基本服务对象；其次，在架构中也较充分地体现了安全服务功能分层摆放、分层提供的特点；再次，安全技术架构也将安全功能涉及的基础支撑平台、基础设施、各种加密安全设备等统一纳入其中，使得安保平台系统更加体系化、系统化。另外，除了加强对安全设备的统一管理外，还需要更新、新增或定制一些必备的安全设备。这些设备，一方面丰富了整个 C 行的安全体系，另一方面，也将 C 行新综合业务系统的安全等级提到了一个新的高度。

在这里谈到设备定制，不能不说到加密机，特别是柜面终端加密机模块的定制。因为这一方面充分体现 C 行大胆创新、敢为天下先的精神。所谓大胆创新，是指使用终端加密模块的方式，从而使柜面系统的安全性有了进一步的提升；所谓敢为天下先，是指大胆采用了 CPK 密码技术，从而开辟了使用国产自主知识产权的密码技术的先河，并得到了密码主管部门的认可。同时，整个设备定制工作也通过了银行界知名专家的技术鉴定。

经过这个阶段项目组成员的辛苦努力，安保平台的基础功能，即设备与密钥安全服务及管理系统、用户与权限服务及管理系统、各种基础设备、KMC 密管中心等模块已经就绪，达到了支撑部分应用系统上线的预期目标。

3）系统功能升级阶段。风险问题、系统稳定性问题是项目组极为重视的问题，因为稍有不慎就会酿成灾难性后果，这主要是基于安保平台的特殊地位。正是基于这样的理念，在此阶段，要重点对安保平台的一期版本进行针对性的风险治理。其过程包括组织有关专家针对性地对安保平台进行甄别、代码审核，并归纳潜在的风险类别；针对风险点逐一进行调整和改进；对已上线系统的影响降为最小。

4）模块调整、模拟演练和上线准备阶段。在此阶段是对安保平台的各种服务功能和管理功能进行针对性的优化组合，以支撑新综合业务系统的分阶段上线需求。为保障上线后系统的稳定运行，应组织全行范围内的模拟演练，并保证系统的稳定性。

5）基础设施扩充及完善阶段。作为整个 C 行信息科技系统的重要支撑模块之一，安保平台的基础设施功能将在此阶段不断得到补充和完善，根据业务发展需求扩充支持服务，如短信 OTP 认证支撑功能、IC 卡密钥管理功能等。

3. 安保平台取得的主要成果

1）体系化建设。C 行安全服务保障平台的建设，不仅仅是一个产品或系统的建设，更是一个安全体系和应用安全架构的建设。一方面，安保平台的设计和建设是依托于 C 行业务应用架构，并对现有系统进行全面而有效的分析后，提炼出来的功能齐备的并为所有业务应用服务的安全服务保障机制支撑平台；另一个方面，安保平台的建设也体现出了安全问题是渗透到各个方面的全局问题，需要在整体上综合考量的思想。有了这样的思想和体系，密码应用和用户安全问题的考察点位置提升了，解决问题的方向更加明确了，应用安全的具体实施方法也就更加便捷了。

目前安保平台体系化成果初露端倪，即依托于 C 行的安全技术架构，构建起了安全基础设施平台、用户安全平台及客户安全平台等三大平台系统。其中安全基础设施平

台是基础并支撑后两个平台，包括安全的基础服务、安全设备及密钥服务等；用户安全平台则侧重服务于行内员工为用户的各类应用系统，主要提供对用户的标识管理、认证支撑功能；而客户安全平台则主要服务于银行客户为用户的应用系统，如网络银行系统、电话银行系统等。用户安全平台和客户安全平台具有许多相似性，但主要差别在于服务于不同用户对象。

2）自主创新成果。安保平台的建设既是技术创新、又是体系创新。安保平台的核心均采用和支持我国密码专家自主创新的算法及体系；同时，应用安全架构也采用了其他同类机构从未采用过的应用安全模式，这些都体现了 C 行积极探索勇于创新的开拓精神。

3）合规性、标准化建设。安保平台的建设与实施有效提高了整个新综合业务系统的安全等级和安全强度。安保平台建设的根本目标，是针对业务应用系统中处理或传输的各类敏感信息处理过程，将敏感信息进行分类，在相关国内、国际安全标准和规范的指导下，提供针对性的安全服务保障处理机制和手段，使得整个业务系统的安全等级或强度充分可调和可控。

4）完善了应用安全风险管理体系。安保平台除了全局化、体系化、有针对性地构建相应的安全服务功能外，也同样充分考虑了安全服务、安全设备及相关密钥的综合管理。在安保平台安全服务、安全设备的管理做到了可集中配置、可集中管理和监控，克服了管理信息分散杂乱的局限性。同时，也将管理安全服务功能所使用的相关密钥复杂性彻底屏蔽掉，并简化与应用的接口，从整体上方便和强化了安全管理工作。

5）完善了 C 行信息系统的安全产品线。安保平台系统的建成，首先将银行传统交易安全功能（PIN/MAC）实现硬件化，并扩充了金融加密机的应用边界，开发和扩充了多种加密机设备类别，包括支持 CPK 功能的加密机、终端加密机模块、通道应用加密机等；其次，实现了对各种安全设备的统一设备管理和密钥管理；第三，建立或完善了认证基础设施，如 PKI/CA/RA 或 CPK/KMC；第四，通过客户安全平台或用户安全平台提供了较为强大的 ID 管理及认证支撑功能，并支持多种认证手段，如口令、CPK USB Key、PKI USB Key、SMS OTP、Token OTP、指纹等；第五，通过用户安全平台提供了重要的 C 行机构数据管理及基于用户的权限管理。

23.2 基于大数据的网络安全态势实践

某股份制银行 M 行，于 2013 年在讨论如何面对 APT（高级持续威胁）攻击时，决定在现有防护技术的基础上，建立基于大数据的网络安全态势体系。

23.2.1 当时的状况和问题

M 行的信息技术环境主要分为互联网域、办公域和生产域两大网络，具体为：

1）办公网：包括支持办公系统的区域和办公网包括分支机构，都通过集中的核心交换机互联后访问互联网。

2）生产网：包括生产系统的区域和互联网出口。

3）安全措施：都是采用双层防火墙架构；所有对网络设备和生产服务器的维护，都要通过堡垒机进行。

虽然在办公网、生产网和分行都采取了多种安全控制措施来保障整个网络的安全性，但是随着飞速发展的互联网安全技术必须采取更为先进的安全控制及管理措施来开展网络安全建设工作，进过对当时状况的分析得出以下问题。

1. 基础安全信息的可视化能力不足

当时的安全控制措施，如防火墙、IDS、终端安全管理系统等，都独立维护和监控，都是一个个信息孤岛，信息不共享，无法关联分析。而且，目前的安全控制措施都是基于签名的方式进行安全检测和防护，只能防范已知攻击，产生的安全日志信息也是基于签名的方式，对于“零日”攻击无法识别。基础安全信息来源不足，内容有限，极大限制了进一步进行安全信息挖掘的能力，需要收集更多的安全信息，为进一步分析挖掘提供基础数据支持。

2. 安全智能分析和感知能力不足

随着业务的增长，安全信息海量增长并呈现非结构化的特点，彼此关联显性不足，目前缺乏强有力的技术手段来支撑信息的采集、分析挖掘和动态感知。需要大数据处理和分析平台，支撑海量信息的处理，需要智能分析模型，快速识别攻击行为和内部用户的违规行为。同时需要引入外部智能知识库，纳入到内部安全分析，以提高效率和准确性。

3. 基于信息技术风险的可视化能力不足

目前主要基于安全事件进行监控和处理，尚无法达到通过风险来衡量信息技术系统的安全状态和趋势。风险是动态的、无法消除的，风险可控是信息技术系统安全的目标。

4. 安全响应和运营能力不足

目前人员组织不足，更不具备安全监控、调查分析取证和响应处理的技术支撑平台，一旦发生安全事件，响应周期会很长，造成的安全损失不可控。

5. 无法有效度量安全管理制度和策略的执行及合规情况

安全合规的可视化水平不足，无法度量安全制度和策略在操作层面的执行及合规情况。

6. 无法有效度量信息技术风险对业务的影响

安全违规事件、攻击威胁事件和信息技术风险的感知处理，到底在多大程度上影响业务，目前不可知，需要通过和业务信息资产、业务目标关联，来进一步判断信息技术风险对业务的影响。

23.2.2 解决问题的思路

针对安全管理体系的规划和发展，M 行以“安全管理成熟度模型”作为安全管理平台规划和建设的指导方法，如图 23-1 所示。

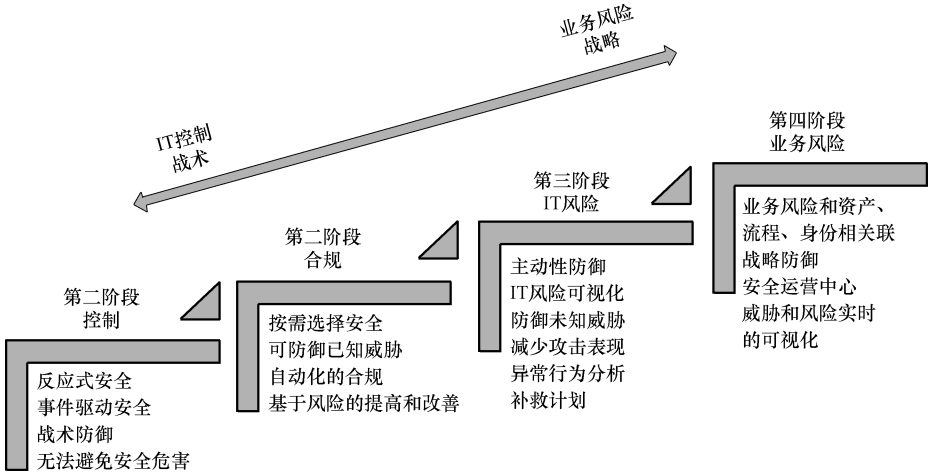


图 23-1 安全管理成熟度模型

该模型主要分为四个阶段，从基础的安全控制阶段，逐步发展到基于业务风险的全面管控阶段，从反应式的安全战术防御阶段，发展到基于业务的战略防御阶段。四个主要阶段的内容如下：

1）第一阶段：控制防御阶段。该阶段处于安全管理水平的初级阶段，是反应式安全，主要靠事件驱动开展安全工作，发现了安全威胁，并造成了一定的损失后，开展安全防护补救。该状态导致安全威胁不可知，事后补救，往往无法避免安全危害的产生。

2）第二阶段：合规管理阶段。该阶段具备安全管理框架和防御体系，可以按照需求选择安全控制措施，部署专业的安全控制措施可实现对已知威胁的检测和有效防护，如部署了 IDS 可检测已知攻击行为、部署了防病毒可检测已知病毒行为等。安全检查和合规在一定程度上可以通过技术手段自动化开展。总体来讲，这仍属于被动防御能力阶段，风险可视化能力依旧不高，无法主动发现安全威胁、主动采取措施，不具备防御未知威胁的能力。

3）第三阶段：信息技术风险管理阶段。该阶段通过采用先进的安全技术，全面整合资源，可全面提高安全信息采集和分析挖掘能力，可以在现有控制措施的基础上，实现更全面、更深度、更智能的安全感知能力。能够有效识别未知的安全威胁和用户异常行为，快速响应和补救，降低安全损失。该阶段以信息技术风险为视角，通过基础数据的采集和分析建模，呈现信息技术风险的可视化。

4）第四阶段：业务风险管理阶段。该阶段将信息技术风险和业务资产、流程、身份进行关联建模，体现信息技术风险对业务可能造成的影响，全面展示信息技术风险的控制能力对业务发展的保障和改善能力，全面提高威胁和风险识别的实时可视化能力。

建立安全运营中心，基于安全分析技术能力，完善人员组织、流程设计，确保业务风险能够快速识别和处理。

安全管理成熟度模型的发展过程，可作为 M 行安全管理平台规划和发展的理论指导。根据当时的状况和存在的问题，M 行信息技术系统已经具备相对成熟的安全管理制度和对应的安全控制措施，形成了以防御和审计为主的安全控制框架。和“安全管理成熟度模型”对标分析，可以认为 M 行的安全管理能力目前处于第二阶段，已经具备了向第三和第四阶段发展的条件。

M 行根据自己的具体情况，选择向第三阶段和第四阶段同时横向发展，然后纵向分步的思路进行建设，而非完全按照成熟度模型定义的分阶段进行映射覆盖。

第一步：建立高级安全运营中心，实现基础信息库和分析、响应能力。建立基础安全信息智能分析平台，能够采集和处理所有的安全信息、同时具备智能分析和挖掘能力，为信息技术风险分析建立数据基础；建立安全事件运营和响应机制，借助安全分析技术平台，建立安全事件响应和运营机制，通过人员组织、流程设计，实现安全运营的初级阶段；建立基于业务的信息安全资产库，将安全事件和业务资产关联，以业务的视角去分析安全事件造成的业务影响。

第二步：逐步完善信息技术风险管理能力，与业务目标建立上下文关系。逐步完善信息技术风险管理相关能力，如策略管理等；以业务信息安全资产库为中心，信息技术风险与业务目标的上下文关联关系，进一步提高安全运营和响应能力。

第三步：将“治理”“合规”“风险”三位于一体。逐步完善信息技术风险管理能力、安全合规能力、操作风险能力，整合基础数据、安全模型、管理制度、风险指标、业务目标等多种资源为一体，建立全行 GRC 平台。

23.2.3 具体方案

1. 安全管理平台总体规划

具体方案如图 23-2 所示。

如上图所示，该架构是 M 行未来安全体系框架的总体蓝图，最终希望能够建成适合 M 行的 GRC 平台，控制和指导全行的信息安全工作。该平台主要有以下部分组成。

（1）安全基础数据源 该平台能够采集网络数据包、安全日志、NetFlow 和终端恶意软件发现类数据，作为整个平台的信息安全基础数据源，为处理和分析挖掘提供数据基础。

（2）数据采集和处理 针对不同的类型，通过不同的方式进行数据采集，采集后，对数据进行解析，根据安全智能知识库和外部信息进行数据富集，建立数据索引，为检索和分析建立结构基础。

（3）安全智能分析、感知和调查 采用大数据分析技术对数据进行挖掘，通过关联分析将各种不同类型的数据源，如网络数据包、日志、终端类数据等，统一进行关联分析，发现潜在的安全攻击和异常行为，产生告警。通过联合调查功能，对安全告警事

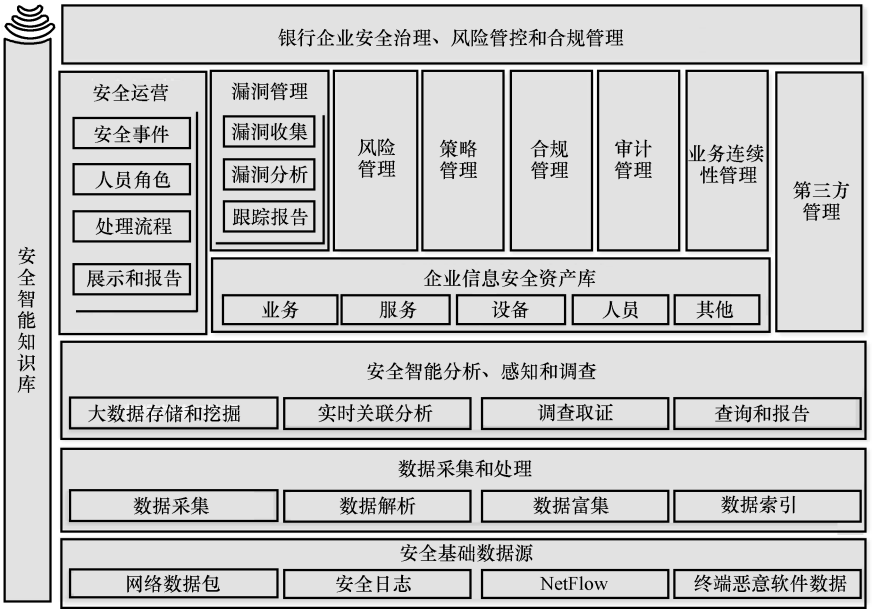


图 23-2　M 行安全管理平台总体规划

件进行调查，找到问题的根源，并可输出报告。

（4）企业信息安全资产库　建立企业信息安全资产库，作为整个安全体系建模的核心，包含了业务、服务、设备、系统、人员等多种信息。利用企业信息安全资产库，可以跟踪产品、服务和业务流程的风险和合规性状态。发现的安全事件可以通过企业信息安全资产库进行信息富集，添加相关的业务上下文信息，如事件所涉及的业务资产、责任人、严重级别等，为安全事件运营、风险管理提供基础模型支撑。

（5）安全运营　基于安全分析产生结果，关联企业业务资产信息，通过人员组织和流程支持，对安全事件进行快速响应和处理，逐步提高运行能力和水平。

（6）漏洞管理　采集各种漏洞扫描系统的扫描数据，与企业业务资产信息库进行关联，对漏洞的分类、影响范围、严重性等进行分析。

（7）风险管理　建立风险目标，基于企业业务资产，将风险目标和漏洞信息、威胁信息进行建模计算，产生风险指标，实现风险可视化，并能够将风险控制在可接受范围内。前瞻性地解决业务所面临的声誉、财务、运营和信息技术风险。

（8）策略管理　为安全策略生命周期的管理提供了一致的流程。将安全管理制度作为管理对象纳入平台管理，实现策略发布、审阅、例外、批准等管理流程的自动化，并能够将策略和业务资产、基础控制措施进行关联，度量策略的执行情况。

（9）合规管理　将内部和外部的安全管理标准、规范和具体控制措施建立映射关系，实现合规的自动化、常态化度量。

（10）审计管理　可以完整控制审计项目的生命周期，实现持续向前的审计优化治理。集中定义审计计划、优先级、流程跟踪和报告，实现自动化审计，提高协作能力和效率。

（11）业务连续性管理　定义业务联系性标准、计划和流程，进行日常业务连续性

测试。

（12）第三方管理 针对第三方合作伙伴进行风险管理和监控、合规管理。

（13）安全智能知识库 建立和维护安全智能知识库，将外部智能库和运营知识库相结合，提供全球安全数据、产品更新、规则更新，将全球智能知识库和内部安全分析相结合，提高识别和感知能力，提高态势感知和预警能力。

2. 完成目标的 3 个阶段

（1）第一阶段 要完成的目标是以下内容：

1）采集网络数据包和安全日志两种类型的数据。

2）数据采集和处理。

3）安全智能分析、感知和调查。

4）企业信息安全资产库。

5）安全运营。

6）漏洞管理。

该阶段注重基础功能的建设实现和运营架构的组件和经验积累，是基础建设阶段。第一阶段的平台建设目标见图 23-3。

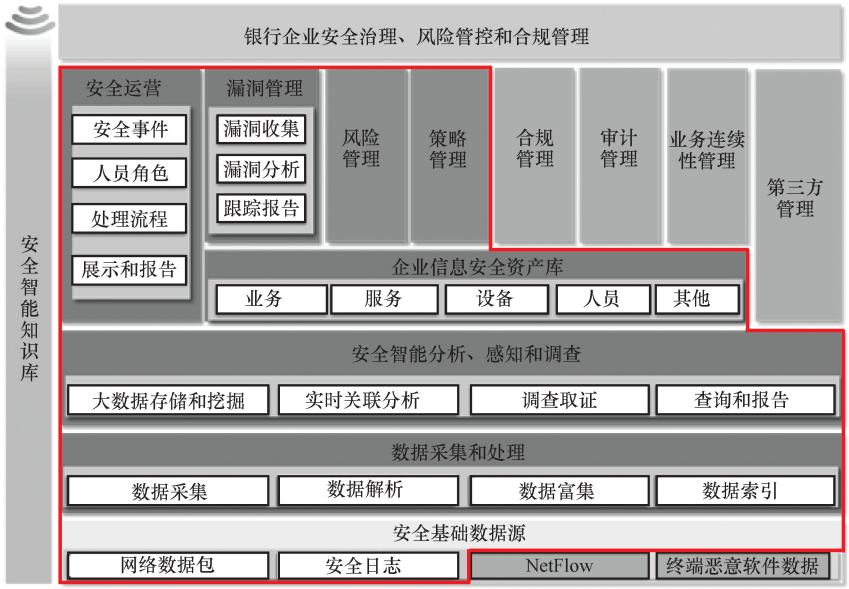


图 23-3 第一阶段的平台建设目标

（2）第二阶段 第二阶段的项目建设主要实现以下内容：

1）数据采集增加 NetFlow 和终端恶意软件扫描数据。

2）风险管理。

3）策略管理。

4）合规管理。

在第一阶段的基础上进一步提高风险可视化能力和合规管理能力，进一步提高安全

运营的效率。第二阶段的平台建设目标如图 23-4 所示。

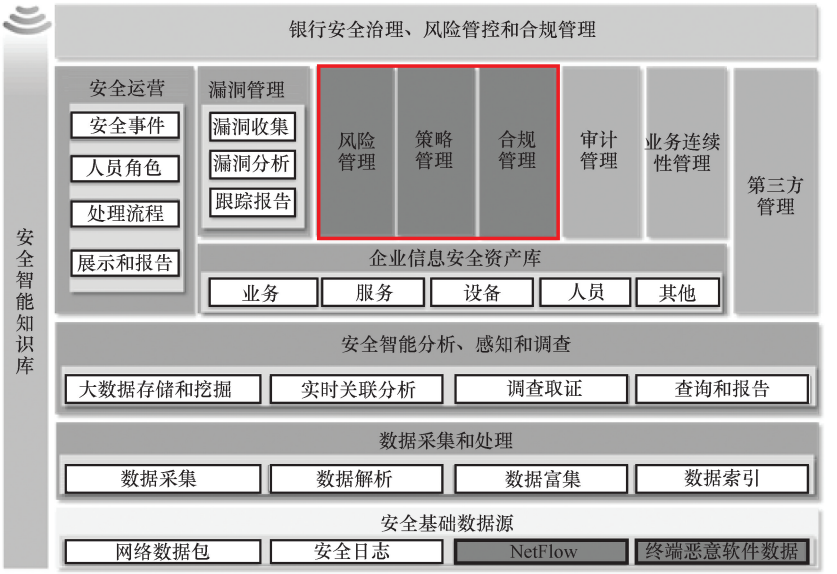


图 23-4　第二阶段的平台建设目标

（3）第三阶段　第三阶段的项目建设主要实现以下内容：

1）审计管理。

2）业务连续性管理。

3）第三方管理。

整合所有功能和资源，全面实现 M 行企业 GRC 平台。第三阶段的平台建设目标见图 23-5。

23.2.4　实际达到的效果

经过 3 个阶段的项目建设后，总体实现了 5 个方面的能力提升，分别如下：

1. 资源整合能力提升

整合全部安全资源，做到安全信息的集中采集、分析和统一管理。

2. 技术能力提升

提高安全分析和感知能力，能够有效发现已知、未知攻击，识别用户的异常、违规行为。提高安全分析的自动化能力和可视化能力，推动安全工作常态化。

3. 控制能力提升

通过富足的信息采集和分析，可以大大提高信息技术风险可视化和合规管理水平。

4. 管理运营能力提升

建立安全的运营体系，提高组织协调能力和快速响应能力，推动安全工作的常

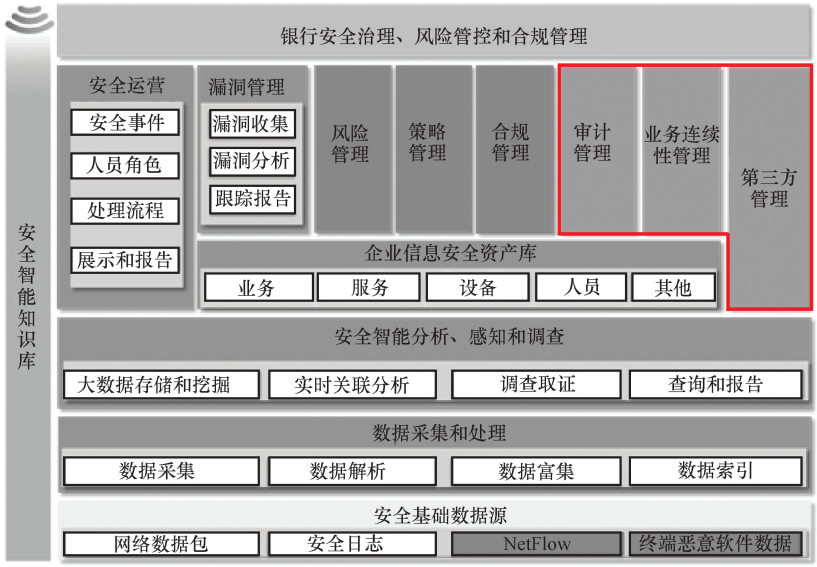


图 23-5　第三阶段的平台建设目标

态化。

5. 业务支撑能力提升

通过建立业务信息安全资产库，将信息技术风险和业务资产进行关联，从业务视角对风险进行管控，提高安全对业务的支撑能力。

安全态势感知技术是银行业加强安全管理，让管理更深入、更主动的关键环节，需要充分理解自身在管理方面的需求，合理选择安全态势感知技术。

23.3　同城双中心灾备建设实例

某股份制银行 A 行为响应建设灾备体系的监管需求，结合本行的实际情况，将数据中心的迁移与同城双中心灾备建设有机结合在一起，成功建成同城双中心灾备体系，详细情况如下。

23.3.1　生产中心信息技术架构整合实践

在建设过程中，根据自身特点，提出了生产中心信息技术架构整合方案，并对之进行了实践。内容如下：

分析业务对信息技术架构服务连续性的要求，建设同城高可用中心、异地灾备中心及开发测试中心的总体建设路线。

将银行业对系统安全的要求，以及业务服务时间的要求，制定安全的、合理的、将生产中心整合到一个生产中心的迁移实施路线。

在迁移过程实施中，充分考虑到业务对信息技术架构的非功能性需求，包括性能、安全、管理、高可用等因素，以及数据中心场所的客观因素，确定机房空间布局的规则，制定整体信息技术物理架构整合方案，实现机房整合。

同时结合信息技术的发展，采用云中心先进的理念，定义资源，形成资源池；以服务目录的形式，对业务提供信息技术基础服务，并完成资源的整合，优化资源的利用率，以此完成计算资源及存储资源的规划及设计。

1. 总体设计原则

生产中心信息技术架构整合总体设计原则，见图 23-6。

图 23-6　生产中心信息技术架构整合总体设计原则

生产中心信息技术架构整合应该首先制定机房整合方案，确定单生产中心的总体建设规划，以及迁移到新生产中心的路线图，确认同城高可用中心、异地灾备中心的规模；并在新生产中心，参考云中心的建设思路，使用标准化、虚拟化、自动化的设计思路，实现资源池与服务目录的使用，完成计算资源规划设计、存储资源设计。

所有的规划设计，都需要考虑银行数据中心的建设准则——安全性、可扩展性、可管理性、高可用性，为实现 COBIT 第五级信息技术服务连续性成熟度做好信息技术建设的基础。

2. 机房整合原则及实践

根据 A 行建设总体演进路线，结合 A 行战略发展和信息技术整体规划，基于以下原则制定 A 行生产中心信息技术架构整合策略：

1）以业务发展战略和信息技术发展战略为指导。

2）参照国际业务连续性最佳并实践借鉴同行经验。

3）基础架构规划充分考虑前瞻性。

4）遵循国家相关监管机构要求及行业管理规范。

5）技术可行与风险成本平衡。

6）统筹规划、分步实施。

目前 A 行生产中心有多个数据中心，包括 6 个在用数据中心、1 个在建数据中心，以及 2 个规划数据中心，生产中心信息技术架构整合的步骤如下：

第一阶段：将非核心系统迁移到较新的数据中心。

第二阶段：以全新的数据中心建设思路，建设 A 行自有的数据中心，并参考云中心等先进的信息技术设计理念，完成信息技术基础平台和计算资源和存储资源的设计，同时完成同城灾备（较新的数据中心）能力的搭建。

第三阶段：将核心系统迁移到全新的生产中心，核心系统自动拥有同城灾备能力，而非核心的迁移也因此而变得安全、可控。

第四阶段：建设全新的异地灾备中心。

通过 4 个阶段的建设，将业务系统整合到新的数据中心；由于新数据中心在建设时，采用新的设备，以及安全冗余的硬件平台，这将提升整个 A 行信息技术系统业务的连续性。同时采用了同城双中心的设计，将业务系统的主系统分布在两个中心，根据不同等级的应用，确定部署比例，并采用应用双活、数据库双活的架构，充分利用，有效地降低成本；完善异地中心的建设，提升业务连续性。

3. 计算资源规划设计及实践

根据同行的经验，以及当前的信息技术的发展，参考云中心的建设思路，应对 A 行业务应用快速增长、灵活变化的需求，未来 A 行生产中心中的服务器架构——计算资源，将采用“资源池”的建设模式，根据业务应用的需求，快速灵活的部署，迅速响应应用计划或突发的计算资源要求。

对于 A 行使用计算资源池的架构设计时，需要考虑现有数据中心整合到新数据中的迁移工作，需要确立以保障应用系统在新数据中心稳定运行为“第一原则”，应尽可能降低由于计算资源架构变化产生的风险。因此，在应用系统迁移过程中，应采用逐步、小规模应用推广计算资源池架构的策略，采用原有物理机加虚拟机的混合模式，以降低风险。

在生产中心的计算资源规划设计遵循保障搬迁的原则、标准化的原则、资源整合的原则、控制风险的原则、可用性的原则、可扩展性的原则、可管理性的原则。

根据上述的设计思路，A 行的生产中心规划设计都从资源池设计开始，包括逻辑层面和物理层面。对于 A 行多生产中心计算资源逻辑部署层面，采用资源池与高可用相结合的方法。实现过程如图 23-7 所示。

根据 A 行的情况，以及对整个信息技术行业的发展，基本的资源类可以分为：X86 虚拟化资源池、Power 分区资源池、HP UX 裸机资源池、Solaris 逻辑资源池、X86 裸机资源池、Power 虚拟化资源池、Power 裸机资源池、X86 大数据资源池、PureScale 资源池，如图 23-8 所示。

结合各个数据中心的机房环境、网络基础架构、存储基础架构等，可以定义每类资源池在不同数据中心的最小部署单元（以机柜为单位）、最大部署能力及扩展的规则。

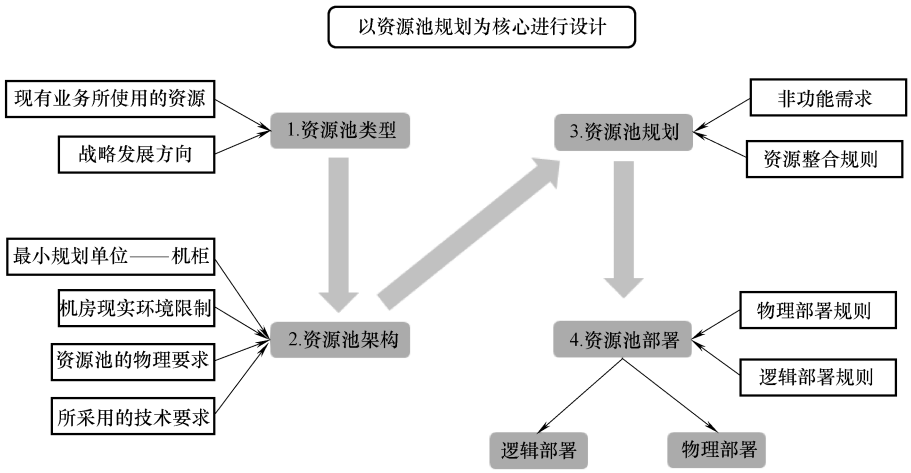


图 23-7　实现过程图

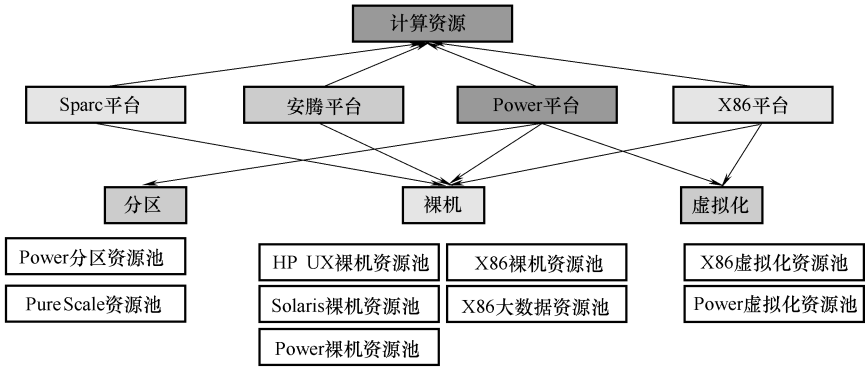


图 23-8　资源类划分

可在每个数据中心内部，以及多个数据中心之间，定义相同类型资源池的关系；在最小的部署单元，完成低阶的信息技术基础架构高可用规划。

在上层应用分配资源时，不用考虑底层的物理设计，便提高规划和使用的可靠性，加快系统建设的效率，完备资源的生命周期管理，提升整个信息技术环境业务连续性的建设。

4. 存储资源规划设计

银行的核心是数据，信息技术系统的业务连续性是以数据为核心的。为了严格保证数据安全，采用以存储和核心，建立 Fabric 的思路：

1）整合存储，根据业务等级的分类、容灾的级别、性能要求等，制定统一的存储使用规划。

2）采用服务目录的形式，对外提供服务。

3）结合 A 行的管理流程，定义决策树。

4）保证灵活性，每套存储支持两个机房的主机访问。

5）优化主机存储的使用，减少灾备复制卷。

6）为存储虚拟化预留足够的接口。

生产中心、同城中心、异地中心的存储，通过存储的复制技术连接到一起，为系统连续性提供重要技术平台。

23.3.2 同城一体化数据中心实践

为了实现 A 行数据中心快速灾难恢复能力和单系统的同城切换能力，同时提高灾备资源利用率和降低灾备投资，在灾备网络建设过程中，采用同城一体化数据中心方案，具体内容如下：

A 行的新生产中心的建设思路都是采用了云中心的设计理念，使用了资源池和服务目录的先进思想，对计算资源和存储，规划不同类型的资源池，确定对应类型的服务目录；并抽象管理运维流程，确定相同服务，不同类型资源池的实施流程，根据每个技术的不同，利用自动化或手工的实施步骤，建立服务标准化的流程，对资源使用者提供单一服务目录界面。

对于可水平扩展的应用所使用的资源，非常适合现有的云中心管理工具。信息技术工具的成熟度非常高，可以采用相应的平台或工具，建立同城一体化虚拟中心，分为用户管理、资源池管理、服务目录管理、门户流程和部署平台、运营监控和分析、资源使用和容量 6 大模块，如图 23-9 所示。

图 23-9 同城一体化

云计算的核心技术是虚拟基础架构技术，在选择基础架构技术时，需要充分考虑到银行数据中心的要求——安全、可靠、可管理的要求，选择信息技术领域内成熟的商业产品。

在虚拟基础架构之上的为云计算引擎。云计算引擎是按云计算需求的把资源池进行逻辑封装的定义，包括用户策略驱动的多租户定义、不同等级资源的逻辑数据中心、网络定义、和服务目录定义等内容。对于以上的资源池、服务目录管理，可以根据虚拟基

础架构，选择云计算引擎。

而云平台的管理界面，也称为门户，可以用来隔离后端不同平台部署的复杂性，带给使用者很多便利，由于需要结合 A 行的管理流程，需要进行二次开发，或者选择接口丰富的产品作为云平台的门户。

对于同城中心双中心，采用同一个的管理界面/系统，建立同城一体化虚拟化数据中心。而异地主中心及其他中心采用自有的管理界面/系统。

将同城一体化虚拟化数据中心纳入资源池的管理模式，在部署时，遵守计算资源的物理部署规则，从物理层面实现高可用；逻辑层面，使用统一的管理规则，实现应用级别的高可用，并最大程度的实现在线动态迁移功能、宿主机硬件高可用、动态资源调配、备份、基于存储的动态资源调配、存储/网络 I/O 控制。这些功能的完善，将有利于 A 行多生产中心的信息技术连续性建设。

23.3.3 同城双中心一体化网络实践

为了实现 A 行数据中心快速灾难恢复能力和单系统的同城切换能力，同时提高灾备资源利用率，在 A 行灾备网络建设过程中，提出了同城双中心一体化网络方案，具体内容如下。

1. 一体化网络建设内容

A 行同城容灾网络环境的设计和建设、演进以服务业务系统为根本目标，充分结合实际环境条件和自身发展规划，选择了一种稳健、前瞻的模式。容灾网络环境主要包括三方面内容：

1）构建数据中心互联（DCI）层面，实现数据中心间简单互联，并支持演进到多数据中心弹性互联的模式。

2）构建承载层面，实现业务对外交付的有效通道。

3）结合内外部环境特点，建设由多运营商组成的双环密集波分（DWDM）传输层面，为网络、存储提供稳定的基础设施。

2. 一体化网络架构设计及实施

一体化网络实施如图 23-10 所示。

（1）构建数据中心互联（DCI）层面 选择支持 OTV、EVI 等 Overlay 技术的 DCB 设备构建数据中心互联环境，在数据中心内部采用 VPC、VSS、IRF2 等技术消除环路，提高链路利用率。在 DCB 设备上隔离两个数据中心的 STP 域，降低单中心环路的影响。根据现有规划，未来 5 年内可能在北京建立一个新的自有数据中心，使用 Overlay 技术可以实现多中心对接。

（2）构建承载层面 使用承载网简化同城数据中心和同城机构、异地容灾中心和分支机构间的层次，实现容灾切换时的流量调度，进而对现有业务流量进行优化。

（3）构建传输层面 传输层面关注两个指标：传输延时，这个指标与链路长度相

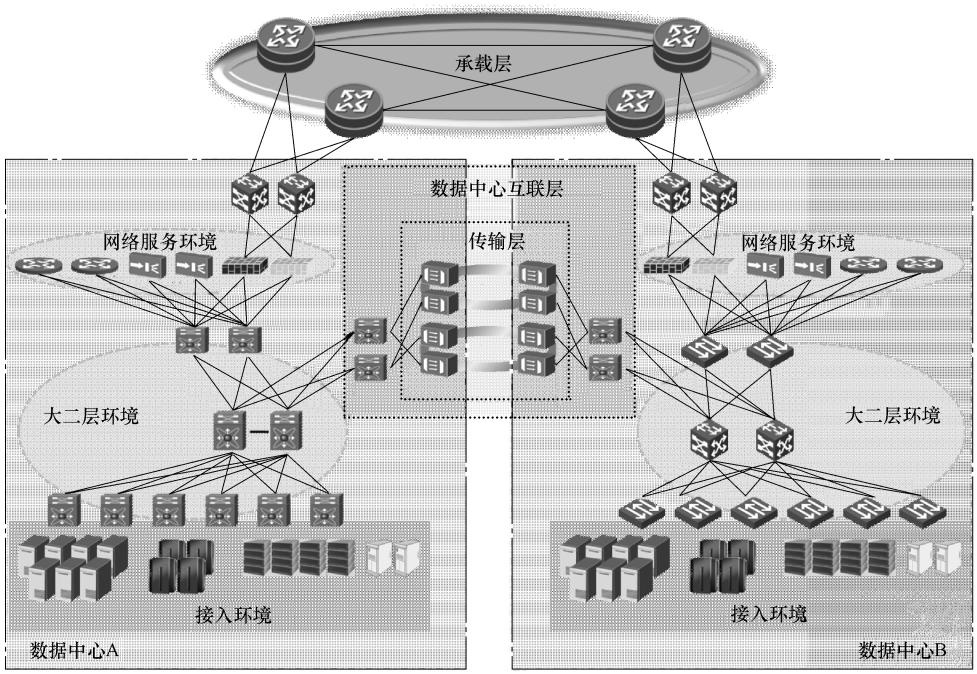


图 23-10　一体化网络实施图

关；稳定性，这个指标涉及的因素较多，都可能对同城环境的可用性造成致命影响。

由于同城数据中心位于郊区，运营商裸光纤（Dark Fiber）资源相对匮乏，且运营商在郊区的维护能力较城区薄弱。为克服这些情况造成的影响，经过多次优化，最终将裸光纤距离控制在 60～70km 之间，将同城系统间延时控制在 1 毫秒以内。采用 3 家运营商 4 条裸光纤实现双环路组网的模式，降低不稳定性因素造成的影响。

另外，在数据中心内使用大二层拓扑来提高资源利用率，使用网络设备的同城集群功能提高业务发布、切换的自动化水平也是本次同城容灾网络建设的具体实践措施。

23.3.4　应用系统双活实践

为了实现 A 行数据中心快速灾难恢复能力和单系统的同城切换能力，同时提高灾备资源利用率，在 A 行灾备建设过程中，提出了应用系统双活方案，内容如下。

1. 应用系统分析

为了能实现真正意义上的双活中心，在 A 行进行了深入研究和探索，其中对 DB2 的 GDPC 双活技术进行了反复的方案验证，最终实现在计费系统上做了 Active-Active 的双活落地实践。该系统的主要特点为：

1）7×24 小时 OLTP 应用，对可用性要求较高。

2）应用类型单一，读写比例较大。

3）功能独立，系统发生异常不会影响全行其他交易。

2. 技术实现分析

GDPC 同城双活技术，即地理上分散的 DB2 pureScale 集群。GDPC 架构允许分布式 DB2 pureScale 集群，从而可以使集群的成员位于不同站点，实现跨数据中心的数据库双活。

构建在标准 DB2 for z/OS® Parallel Sysplex®的数据共享体系结构上时，DB2 pureScale Feature 在 AIX®和 Linux 平台上提供了突出的数据库可伸缩性、可用性和应用程序透明性。但是，任何单一站点系统（甚至是 DB2 pureScale 系统或 DB2 for z/OS Parallel Sysplex）都容易受到会危及整个站点安全的外部事件（例如，大范围的电源或通信中断）的攻击。因为灾难（如电源故障和火灾）可能会禁用单个数据中心，所以许多大型 信息技术组织都配置了 2 个站点，这足以应付单独的电源线路故障。此配置将使整个系统中断的风险降至最小，并允许在一个站点上开展业务，即使另一个站点受到灾难的影响时也是如此。与 DB2 for z/OS 的 Geographically Dispersed Parallel Sysplex™配置一样，地理上分散的 DB2 pureScale 集群也提供了常规单一站点 DB2 pureScale 集群的可伸缩性和应用程序透明性，而在启用了 Active-Active 系统可用性的跨站点配置中则未提供，即使面对许多类型的灾难也是如此。

双活 Active-Active 的工作模式非常关键，这是因为它意味着在正常操作期间，2 个站点中的 DB2 pureScale 成员将照常共享它们之间的工作负载，并进行工作负载均衡（WLB），以使站点内或站点之间的活动在所有成员上都保持最佳级别。这意味着第二个站点不是在等到发生某些错误时可用的备用站点。相反，第二个站点正在发挥其作用，即使在日常操作期间也能使投资得到回报。

典型的 DB2 pureScale 集群由下列各项组成：

1）2 个或更多 DB2 pureScale 成员。

2）2 个集群高速缓存设施（CF）。

3）连接了 SAN 并正在运行 GPFS 的集群存储器。

4）低延迟的高速连接，例如，InfiniBand（IB）、10GE 或基于聚合以太网（RoCE）的远程直接存储器存取（RDMA）。

该集群具有 4 个成员和 2 个 CF，并使用 10GE 网络进行等待时间较短的通信。DB2 pureScale Feature 是一种共享数据体系结构，在该体系结构中，所有成员都对数据库的单个副本执行操作并通过 CF 相互通信，以使活动同步及插入、修改和检索应用程序所需的数据。成员与 CF 之间的消息是使用集群互连中的 RDMA 功能，该功能将使通信等待时间极短并使每条消息的 CPU 使用率非常低。在利用了以太网的 pureScale 集群中，存在一些非常有限的成员到成员通信。

在站点 A 与 B 之间将 DB2 pureScale 分割成相等的两半时，意味着半数成员系统将实际位于站点 A 中，而另一半则位于站点 B 中。在发生站点故障情况下，如果要实现 Tie Breaking 和透明故障转移，那么需要第三个站点，即应该在两个主站点中各放置一个 CF，以避免单一故障点（SPOF）。为了保持 DB2 pureScale 软件的最佳性能和可伸缩性，在站点之间使用支持 RDMA 的互联，以便从一个站点中的成员发出的消息能够尽

快且开销尽可能小地到达另一个站点中的 CF。

除了分散计算资源（例如，成员和 CF）之外，灾难恢复（DR）集群配置还要求在站点之间复制存储器。构建在标准 DB2 pureScale 集群设计上时，GDPC 配置在站点之间使用 GPFS 同步复制，以使所有磁盘活动在集群中处于最新的状态，这包括表空间写操作和事务日志写操作。

23.3.5 数据库容灾技术实践

A 行现有业务系统大部分使用了 DB2 数据库，对关于如何基于数据库主机构建双活架构也进行研究和落地实践，HADR 技术在快速的灾难恢复能力上和降低灾备投资上都有一定的优势。对于使用基于数据库复制技术实现异地容灾，A 行科技开发部根据现实情况及监管要求对容灾体系的建设提出以下需求：数据一致性需求、系统高可用性需求、系统性能需求、系统健壮性需求、管理监控需求。

基于以上的需求，A 行科技开发部对 DB2 数据库的 HADR 数据复制技术进行了反复的实践与验证，并逐步总结了关于该技术在实际大型生产系统的落地实践经验。

技术实现分析表明，HADR 是 DB2 中高可用性和灾难恢复的解决方案。通过该解决方案，用户可以为实际生产系统的数据库设置一个备用数据库，前者称为主数据库，后者称为备机数据库。主数据库上的数据更改通过数据库日志传送到备机数据库上，备机数据库通过重做这些日志完成与主数据库上相同的数据更改，从而使两者的数据保持一致。在主数据库发生故障时，用户可以在备机数据库上通过接管 HADR 命令使备机数据库成为新主数据库，业务应用可以运行在新主数据库之上，从而使数据库服务恢复。

根据该技术在 A 行的落地实践，可以发现基于数据库复制技术实现异地灾备的方案，相对于使用其他方式的方案具有以下明显的优势：快速的灾备切换、高性能的数据同步、灵活全面的数据保护、适合异地 WAN 链路、跨越硬件限制、有效利用系统资源、节省灾备投资。

23.3.6 灾备指挥与自动化切换平台实践

为适应中国 A 行科技开发部生产运营发展的需要，降低管理员的大量低效劳动，减少人为操作失误，实现运维工作统一、规范和流程化的管理。在前期业务调研和论证的基础上，启动灾备指挥与自动化切换平台的研究与实践工作，与现有生产系统及容灾架构有效整合，实现同城灾备系统一键式切换。通过灾备指挥与自动化切换平台建设主要解决以下问题：

◇ 手工切换任务烦琐，涉及不同岗位人员，组织、调度耗时较多，影响实现演练的 RTO 目标。

◇ 手工执行切换命令，操作风险较高，影响切换成功率。

◇ 切换操作效果一定程度上依赖命令执行人员对系统的熟悉程度。

◇ 预案和操作手册编写手工管理，管理成本较高。

综上所述，从科技开发部生产运营工作的实际情况出发，建立灾备指挥与自动化切换平台，实现灾备切换的自动化，缩短灾备切换时间，满足灾备中心所有系统、网络设备和存储设备等自动化切换，保证灾难情况下可以实现灾备切换自动化。

1. 平台架构设计

灾备指挥及自动化切换架构设计如图 23-11 所示。

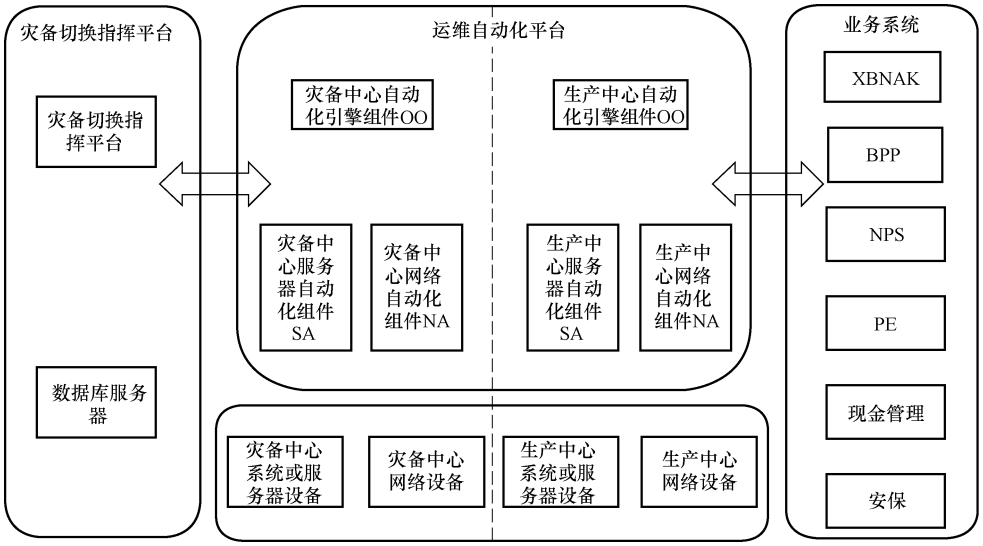


图 23-11　灾备指挥及自动化切换架构设计图

灾备指挥与自动化切换平台整体架构包含四大组件模块，分别是灾备切换指挥平台、自动化引擎组件 OO、服务器自动化组件 SA、网络自动化组件 NA。

2. 灾备切换指挥平台

主要功能是将传统的以表格及静态演练流程图形式记录发布管理整个演练流程，转化为通过系统预设演练流程动态交互管理整个灾难恢复过程，实现灾难恢复演练的工具化管理，大大提升演练步骤开发、管理和变更的效率，让系统恢复、容灾演练更具有可控性和可操作性。整体系统从功能上分为需要包含灾难恢复组织及人员信息管理功能、权限设置功能、工作台功能、流程录入功能、流程执行功能、恢复进度展示功能、日志记录功能、导入导出功能、公告管理功能、DRP 电子化管理功能、系统管理功能等功能模块。

3. 自动化引擎组件 OO

负责灾备切换自动化流程定制，调度和与外部系统的集成。灾备自动化切换流程开发统一由 OO 实现，并实现与灾备切换指挥平台无缝集成。

4. 服务器自动化引擎组件 SA

负责服务器运维自动化的具体功能实现，可以管理各种类型的服务器如 AIX、HP-UX、Windows、Linux 等。

5. 网络服自动化引擎组件 NA

负责网络运维自动化的具体功能实现，可以管理各种网络设备如交换机、路由器、防火墙等。

6. 高可用架构

确保灾备指挥与自动化切换平台高可用性。

23.3.7 同城双中心一体化运维管理体系实践

灾备中心的建设是与本地数据中心紧密结合的，特别是为了提升灾备中心的利用率，运维团队更倾向于建设双活的灾备中心，这使得一体化运维体系成为必然选择。灾备建设中应该考虑到灾备中心对现有运维组织架构、流程制度等的需求，基于一体化运维体系来保持整个生产系统的一致性、可维护性，确保容灾机制快速生效。一体化运维体系一方面可以确保主备环境一致性，特别是确保变更在主备环境下均得到有效实施和验证；另一方面则为容灾提供人员技术保障，确保运维人员熟悉主备环境和操作规范，及时快速地进行容灾操作。

1. 运维管理组织需求分析

运维管理体系一直是银行业信息科技的基础，监管部门非常重视信息科技的稳定运行，行业标准也较为成熟。建设一体化运维体系，可以参照监管机构要求，如《银行业信息科技风险指引》《商业银行数据中心监管指引》《商业银行业务连续性监管指引》等监管指引和行业标准 ITIL、ISO/IEC 20000、ISO/IEC 27001、ISO/IEC 9001、COBIT。结合当前各行的实际情况，在建设灾备体系时，往往都已经建立了较为完善的数据中心管理体系，灾备中心建成后可以融入现有的体系中。通过对现有体系补充完善，实现涵盖两地三中心的一体化运维。

A 行灾备体系建成后，即将灾备环境信息技术对象作为当前生产环境运维管理的信息技术对象的扩展，由生产环境运维组织支撑同城灾备中心的运维，暂不设立独立的灾备运维组织和岗位，只需更改生产环境运维与管理岗位的职责范围。如此，即节省运维费用，又能平滑顺利地实现灾备系统的运维。

2. 一体化运维管理体系建设

一体化运维管理体系重点完善两个方面，一方面是故障发生时的应急机制，要充分考虑到容灾应急预案的执行，应该完善应急值班、应急预案文档，确保人员及时到位，并采取有效措施；另一方面则是加强变更管理，确保配置一致性，保障容灾环境的有效。

3. 一体化监控管理体系建设

目前各商业银行数据中心普遍建立了完善的监控体系，A 行目前的监控体系主要包括机房设施监控、网络监控、网络流量分析平台、系统监控平台、交易性能监控平台

等。灾难发生时，备用数据中心的监控对于保障正常生产至关重要。因此在同城双中心建设过程中需要考虑关键监控工具在同城双中心架构下的部署及容灾设计。

1）同城双中心基础环境、网络和系统平台监控管理解决方案。同城双中心监控管理体系首先考虑正常运行情况下的监控有效性，在成本许可的范围内，对于灾难场景下采用监控服务器热备等方式进行灾难场景下的监控管理连续性。

针对机房设施监控，各数据中心采取独立部署方式，能够独立运行，并且在灾难发生场景下，可用数据中心的机房设施监控不受影响。

网络监控和系统监控平台目前为全国集中的监控方式，采用了多级部署，告警传输双通道的设计，在同城双中心的架构下，采取监控服务器双中心采取热备冗余部署方式。正常情况下，监控采集机将告警及性能数据传递到主数据中心，灾难发生时，启用备数据中心的监控服务器，继续接收各分布式采集机上传的告警事件和性能数据，确保灾难情况下的持续监控。图 23-12 为系统集中监控平台的一个实现架构。

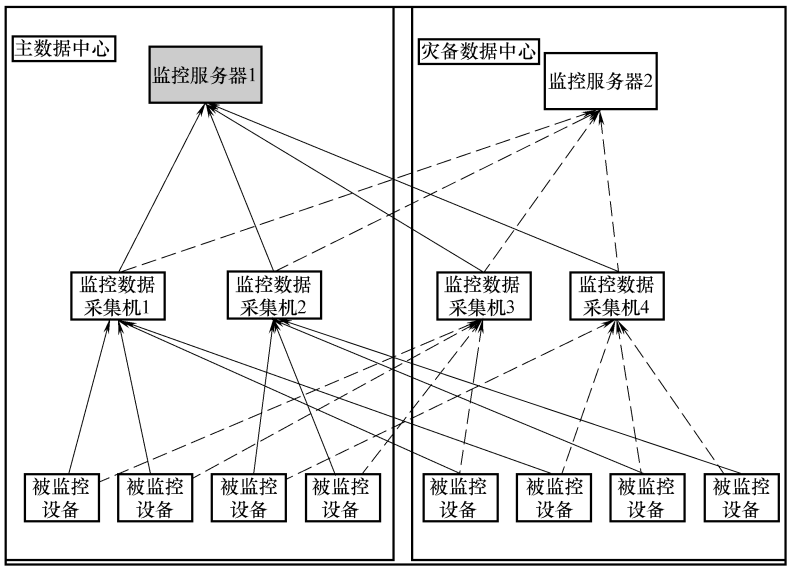


图 23-12　系统集中监控平台实现架构图

目前同城双中心部分应用采取双活模式，日常监控中需要同时监控和处理双中心的告警事件，而应用系统采取逻辑分组的方式，区分生产系统和同城灾备系统的告警。分组界面上的分组呈现，如图 23-13 所示。

2）同城双中心交易性能监控系统解决方案。交易性能监控系统，A 行是采取网络旁路复制流量加交易协议解析的方式实现的。基本架构如图 23-14 所示，包括流量汇聚层和业务可视化分析平台两个主要部分，将告警事件上传至集中监控平台处理。

在每个数据中心部署多台流量汇聚设备，对多个机房、多个监控点的流量进行采集和汇聚，对流量进行分析、过滤处理后，按照一定的原则和要求，将过滤处理后的“干净的”流量输送给业务可视化监控分析平台和交易性能监控平台进行分析处理。

图 23-13　分组界面图

23.3.8　信息技术服务连续性管理体系建设实践

（1）体系建设的内容　为了确保灾备体系随时就绪，在 A 行灾备实施过程中，制定了信息技术服务连续性管理体系建设方案，并对之进行了实践。内容如下：

1）定义了信息技术服务连续性管理的宗旨。

2）定义了信息技术服务连续性管理体系相关术语。

3）定义了信息技术服务连续性管理的基本原则。

4）定义了信息技术服务连续性管理参照的规范。

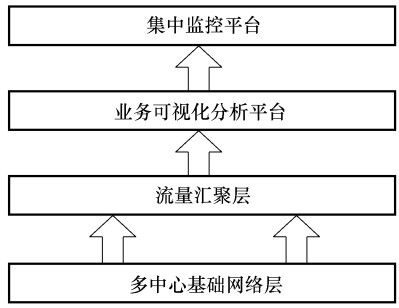


图 23-14　基本构架图

5）定义了信息技术服务连续性管理体系组织架构及职责分工。

6）制定了信息技术服务连续性风险评估管理办法。

7）制定了业务影响分析管理办法。

8）制定了灾难恢复策略开发管理办法。

9）制定了灾备方案规划设计、实施与交付管理办法。

10）制定了灾难恢复预案开发及更新管理办法。

11）制定了灾备演练管理办法。

12）制定了灾备系统测试验证与优化管理办法。

13）制定了应急处置管理办法。

14）制定了业务连续性培训管理办法。

15）定义了信息技术服务连续性管理岗位的日常监测规程。

16）定义了信息技术服务连续性管理岗位的自我评估规程。

（2）体系建设的收益 一般大型商业银行的信息技术系统每天处理着几亿笔金融交易，瞬间交易的丢失可能带来不可估量的资金损失和业务风险。实施双活数据中心模式后，利用站点双活切换机制，可以缩减占全年停机时间95%的计划内停机时间，保障了银行金融交易对账务数据有着严格的实时性、准确性及事务完整性的要求，并且带来以下收益：

1）高效率：提高灾备系统运维效率，缩短灾备切换时间。核心应用系统灾备切换模拟演练比人工操作至少提高5倍。

2）可视化：灾备指挥与自动化切换平台，自动化流程执行可视化和可跟踪，有异常可以及时处理，提升用户体验。

3）流程化：流程标准化减少人工操作风险，规范切换操作流程。预案和操作手册编写手工管理通过灾备指挥与自动化切换平台实现，大大降低管理成本。

参 考 文 献

[1] 雷万云. 信息安全保卫战——企业信息安全建设策略与实践 [M]. 北京：清华大学出版社，2013.

[2] Mark Rhodes-Ousley. 信息安全完全参考手册 [M]. 2 版. 李洋，段洋，叶天斌，译. 北京：清华大学出版社，2014.

[3] 张吉光，梁晓. 商业银行全面风险管理 [M]. 上海：立信会计出版社，2006.

[4] 柳永明，李宏. 商业银行风险管理 [M]. 上海：上海人民出版社，2007.

[5] 李建平，冯吉闯，高丽君. 商业银行操作风险度量与监管资本测定——理论、方法与实证 [M]. 北京：科学出版社，2013.

[6] 才凤玲. 商业银行实务 [M]. 北京：清华大学出版社，2007.

[7] 冯登国，赵险峰. 信息安全技术概论 [M]. 2 版. 北京：电子工业出版社，2014.

[8] 阎庆民，谢翀达，骆絮飞. 银行业金融机构——信息科技风险监管研究 [M]. 北京：中国金融出版社，2013.

[9] 吴翰清. 白帽子讲 Web 安全 [M]. 北京：电子工业出版社，2013.

[10] 向宏，傅鹂，詹榜华. 信息安全测评与风险评估 [M]. 2 版. 北京：电子工业出版社，2014.

[11] 沙梓社，吴航，刘瑾. iOS 应用——逆向工程分析与实践 [M]. 北京：机械工业出版社，2014.

[12] 李建平，李吉闯，宋浩，等. 风险相关性下的信用风险、市场风险和操作风险集成度量 [J]. 中国管理科学，2010，18 (1)：18-25.

[13] 丰吉闯. 商业银行操作风险与系统性风险度量研究 [D]. 合肥：中国科学技术大学论文. 2012.

[14] Michael E. Whitman，Herbert J. Mattdrd. 信息安全管理 [M]. 向宏，傅鹂，译. 重庆：重庆大学出版社，2005.

[15] 丰生强. Android 软件安全与逆向分析 [M]. 北京：人民邮电出版社，2013.

[16] 张尼，刘镝，张云勇，等. 云计算安全技术与应用 [M]. 北京：人民邮电出版社，2014.

[17] 郝玉洁，吴立军，赵洋，等. 信息安全概论 [M]. 北京：清华大学出版社，2013.

[18] 阎庆民. 操作风险管理“中国化”探索——中国商业银行操作风险研究 [M]. 北京：中国经济出版社，2012.

[19] 杜世清. 商业银行操作风险管理实务 [M]. 成都：西南财经大学出版社，2011.

[20] Carrillo S，Czyl H，Tagliani A. Reconstructing heavy-tailed distributions by splicing with maximum entropy in the mean [J]. Journal of Operational Risk，2012，7 (2)：3-15.

银行业信息科技风险管理高层指导委员会简介

银行业信息科技风险管理高层指导委员会（简称高层指导委员会）是由银监会发起，20家主要银行业金融机构自愿参与建立的行业性、专业性高层组织。高层指导委员会的宗旨是：以全面风险管理为导向，提升银行业信息科技核心竞争力和自主创新能力，提升银行业信息化建设和信息科技风险管理整体水平，推动银行业信息科技持续、健康发展，维护金融稳定和国家安全。高层指导委员会的主要任务是对银行业信息化建设与信息科技风险管理工作进行研究、指导并提供咨询、建议，研究银行业信息化建设重大发展问题，深入传导贯彻信息科技监管政策，开展专业指导和风险分析，开展信息科技课题研究，推动银行业信息科技领域新兴技术研究，促进银行业信息科技领域的交流合作。高层指导委员会自2011年成立以来，建立了风险分析、课题研究、专业指导等常态化工作机制，编制了《金融科技治理与研究》期刊，组织开展了近300项课题研究，组织银行业金融机构协同开展安全可控、自主创新能力建设，为银行业信息科技领域的经验交流、知识分享和资源互补提供了有效的平台。

367 1353096356903 0531605312 350

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

银行数据治理

商业银行信息系统研发风险管控

全球化时代的银行信息系统建设

商业银行私有云设计与实现

银行信息系统架构

■ **银行信息安全技术与管理体系**

商业银行业务连续性管理

金融数据挖掘与分析

银行数据中心基础设施建设与运维管理

银行业信息科技监管

地址：北京市百万庄大街22号
邮政编码：100037
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
封面无防伪标均为盗版

机械工业出版社微信公众号

上架指导 金融

ISBN 978-7-111-52252-2

ISBN 978-7-111-52252-2

定价：79.80元