金融IT服务外包
信息安全管理

Information Security Management for
IT Outsourcing in the Financial Industry

柴洪峰 主编

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

金融IT服务外包
信息安全管理

Information Security Management for IT Outsourcing in the Financial Industry

柴洪峰 主编

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

内容提要

本书在回顾国内外金融 IT 服务外包产业的发展历史以及政府监管政策的基础上，结合银联数据服务有限公司的具体实践，从战略层到执行层等多个层面详细介绍了金融 IT 服务外包企业在安全治理和安全管控方面的方法和措施。

本书适合金融 IT 行业特别是金融 IT 服务外包行业的从业人员阅读和参考，也可作为企业信息安全管理从业人员的参考书。

图书在版编目(CIP)数据

金融 IT 服务外包信息安全管理/柴洪峰主编. —上海：上海交通大学出版社，2015
ISBN 978-7-313-12574-3

Ⅰ. ①金… Ⅱ. ①柴… Ⅲ. ①金融—商业服务—对外承包—信息安全—安全管理—研究—中国 Ⅳ. ①F832.6

中国版本图书馆 CIP 数据核字(2015)第 013908 号

金融 IT 服务外包信息安全管理

主　　编：柴洪峰
出版发行：上海交通大学出版社　　地　　址：上海市番禺路 951 号
邮政编码：200030　　电　　话：021-64071208
出 版 人：韩建民
印　　制：常熟市文化印刷有限公司　　经　　销：全国新华书店
开　　本：880mm×1230mm　1/32　　印　　张：4.375
字　　数：86 千字
版　　次：2015 年 1 月第 1 版　　印　　次：2015 年 1 月第 1 次印刷
书　　号：ISBN 978-7-313-12574-3/F
定　　价：28.00 元

前　言

自20世纪90年代以来，在信息技术革命、经济全球化以及市场竞争加剧等因素的共同推动下，包括金融IT服务外包在内的金融信息服务外包产业迅猛发展，金融IT服务外包不仅可以使金融机构专注于核心业务、降低运营成本、最大限度地提高企业效益，也促进了整个金融IT服务外包产业的发展。但是，伴随着信息技术与金融行业的深度融合，在信息安全环境日趋复杂和政府监管日趋严格的背景下，金融IT服务外包的信息安全问题已成为发包方、接包方以及监管机构越来越关注的问题。

信息技术的飞速发展和应用在促进整个金融行业发展的同时，也带来了前所未有的安全威胁，如何在有效利用信息技术的同时，积极规避和应对这些风险，如何保障信息的安全储存、传输和使用，如何实现信息的保密性、完整性、可用性和可控性，是整个金融行业和金融IT服务外包企业共同面临的重要课题，也是整个金融IT服务外包行业持续、健康发展必须要解决的关键问题。

金融IT服务外包行业的信息安全管理是一项系统工程，它

与整个IT行业信息安全管理有许多共通之处，同时也有作为服务外包行业所特有的要求和规范。银联数据服务有限公司作为金融IT服务外包行业的先行者和重要参与者，在公司十余年的发展历程中，积累、探索出了一套适合当前信息安全环境和公司自身实际的信息安全管理体系，本书就是在借鉴整个IT行业信息安全管理体系和方法的基础上，结合自身经验归纳、总结并提炼实际运作方法，希望对整个金融IT服务外包行业的信息安全管理有一定的参考价值。

本书在编写过程中参考了国内外许多同行的论文、著作，在此表示感谢。由于编者水平有限，书中存在的错误和疏漏，敬请读者批评指正。

目　录

第1章　金融IT服务外包信息安全概论

1.1　金融IT服务外包概述

20世纪80年代以来，随着经济全球化、一体化进程的加快以及市场竞争的加剧，作为新兴产业的服务外包在世界范围内迅猛发展，成为企业进行资源优化配置和新一轮国际产业转移的重要推动力，特别是90年代以来信息技术革命浪潮的推进，使外包产业步入了发展的黄金期。金融行业作为一个知识和科技密集型行业也在这一时期开始大规模运用信息技术来支撑其复杂的运营管理体系，提高运营效率，降低运营风险，同时对IT系统的可靠性、可用性、安全性和快速适应性提出越来越高的要求。依靠金融机构自身提供这些服务需要付出大量的人力、物力和财力，出于成本和利益的考虑以及社会分工日益细化的趋势，金融行业开始大量将其信息服务外包给第三方，从而使自己专注于核心业务，降低运营成本，最大限度地提高企业效益。

金融IT服务外包是金融信息服务外包的重要组成部分，金

融信息服务外包又可称为“金融服务外包”。2004 年 8 月 2 日，在巴塞尔银行监管委员会(BCBS)、国际证监会组织(IOSCO)、国际清算银行(BIS)以及国际保险监管协会(IAIS)组织的联合论坛上发表的《金融服务业务外包》文件中将金融服务外包(Outsourcing in Financial Services)定义为受监管实体持续利用外包服务商(既可以是集团内的附属实体，也可以是集团外的实体)来完成以前由自身承担的业务活动。外包可以是将某项业务(或业务的一部分)从受监管实体转交给服务商操作，或由服务商转交给另一服务商(转包)。在这里“受监管实体”指的是发包方，主要包括银行、证券公司和保险公司等金融机构；外包服务商是接包方或者称第三方，外包的范围不包括购买合同，“购买”指的是“从工艺上取得货物、设备和服务，但卖方不转移与客户有关的财产权信息或与其商业活动相关的未公开的信息”。

在不断演变的外包模式中，金融机构和外包服务提供商在长期发展中建立的合作关系也在演变。很多全球金融机构与长期合作的外包服务提供商建立起战略合作关系，利用双方优势，合作共赢。对服务外包持更加开放的态度，同时更全面地评估外包商的实力，可以帮助金融机构最大化外包对提升自身经营、培养核心竞争力所带来的积极作用。金融机构不仅应当将服务商团队的质量作为关键的考量要素，而且应当坚持与高质量的服务提供商进行长期合作。这样的合作关系不仅有助于金融机构以外包模式深化自身业务流程的梳理和提高运营精益化，而且也可以

间接阻碍竞争对手通过类似方式培育能力，从而确立自身的有利竞争地位，这样的战略合作关系对双方都是有益的。

1.1.1　金融 IT 服务外包的类型和模式

金融信息服务外包按照内容可以划分为信息技术外包(ITO)、业务流程外包(BPO)、营销外包、资产管理外包和知识处理外包(KPO)。目前以信息技术外包和业务流程外包为主。金融 IT 服务外包按照不同的划分标准又可以细分为不同的类型。

金融业务流程外包是指金融机构将内部职能的全部功能外包给外部服务提供商，由供应商对这些流程进行运作、管理或者重组。例如人力资源管理、贷款业务处理流程服务、呼叫中心、数据管理、ATM 服务、e-banking 等服务。联合国《2003 年电子商务和发展报告》中有对银行 BPO 的业务详列，内容涵盖银行业务与内部管理众多方面，如支票处理、贷款管理、分类账、薪水津贴、职员招募都可进行 BPO。

银行、证券基金和保险公司都会不同程度地将数据信息的录入与处理业务、呼叫中心业务、财务处理和人力资源管理等业务外包。与此同时，银行还会把按揭服务和信用卡服务，保险公司还会把保单管理、理赔、代理机构管理、核算、精算等自身特有的业务职能外包。金融机构特别适合 BPO，这是由于其某些业务流程的重复性以及烦琐性决定的。以信用卡 BPO 为例，银行可以将

申请表的受理和录入、信息核实、电话征信、账单打印和邮寄、催收等业务外包给第三方，自己专注于信用卡的市场开拓和管理。

金融营销外包在保险行业以及信用卡营销行业比较普遍，是指发包方利用其他机构销售自身产品。这种营销外包主要分两类：一是通过隶属于自己专属的代理机构营销（内包）；二是通过独立的第三方代理机构代销（外包）。

金融资产管理外包是近年来在西方国家发展比较快的一种财务管理模式，是企业将财务管理过程中的某些事项或流程外包给外部专业机构代为操作和执行的一种财务战略管理模式。

金融知识处理外包指金融机构为提升自己的决策能力和专业化运作水平，要求外部服务提供商提供全面、及时、综合的市场判断和研究解释，提供专业的研究结果和解决方案，其中包括数据信息分析、专项业务资讯、投资策略与决策支持、市场风险与评估、技术研究、专利申请等。KPO是外包服务的最高级形式。

1）按照服务内容划分

金融IT服务外包按照内容划分，主要包括系统操作服务、系统应用服务和基础服务三类。系统操作服务如信用卡数据、各类保险理赔数据、税务数据、法律数据等的处理及整合；系统应用服务包含信息工程及流程设计、管理信息系统服务、远程维护等；基础技术服务则有软件开发设计、基础管理平台整合或管理整合等。目前国内的ITO实践集中在将金融数据处理、金融服务软

件与系统开发、金融灾备与清算中心等业务发包。

金融机构的 IT 系统是一个复杂、庞大而又紧密相连的系统架构，是保证金融机构安全有效运转的“大脑”和“神经系统”。以银行的 IT 系统为例（见图 1.1），它包括业务系统、管理信息系统、渠道系统和其他系统，这个庞大的系统单凭银行自身是无法独立组建和维护的，这就需要一些专业的外包机构协助他们组建并不断地完善银行的 IT 架构体系。IT 外包可以使银行在迅速变化的信息时代获得技术上的比较优势和成本优势，这是银行与外部信息技术企业之间资源或利益的交换，这种交换为银行改进价值链提供了机会。

2）按照金融机构与外包提供商之间的股权关系划分

按照金融机构与外包提供商的股权关系，金融 IT 服务外包可以被划分为外包给发包方的全资控股机构、外包给发包方合资机构、外包给直接第三方和外包给非直接第三方等四种形式。

（1）外包给发包方的全资控股机构。

金融机构在本地或其他成本较低的离岸外包目的地建立全资控股外包机构。该方式由于需要较大规模的前期投入，只适用于大型金融机构。因其直接由母公司管理，因此较其他外包方式的风险更低。此外，因不涉及第三方，在其他相同条件下，可以更大程度地节省中间费用。目前，摩根大通、花旗银行和标准人寿等大型金融机构都在印度、菲律宾等公司所在国之外的国家设立了全资外包机构。

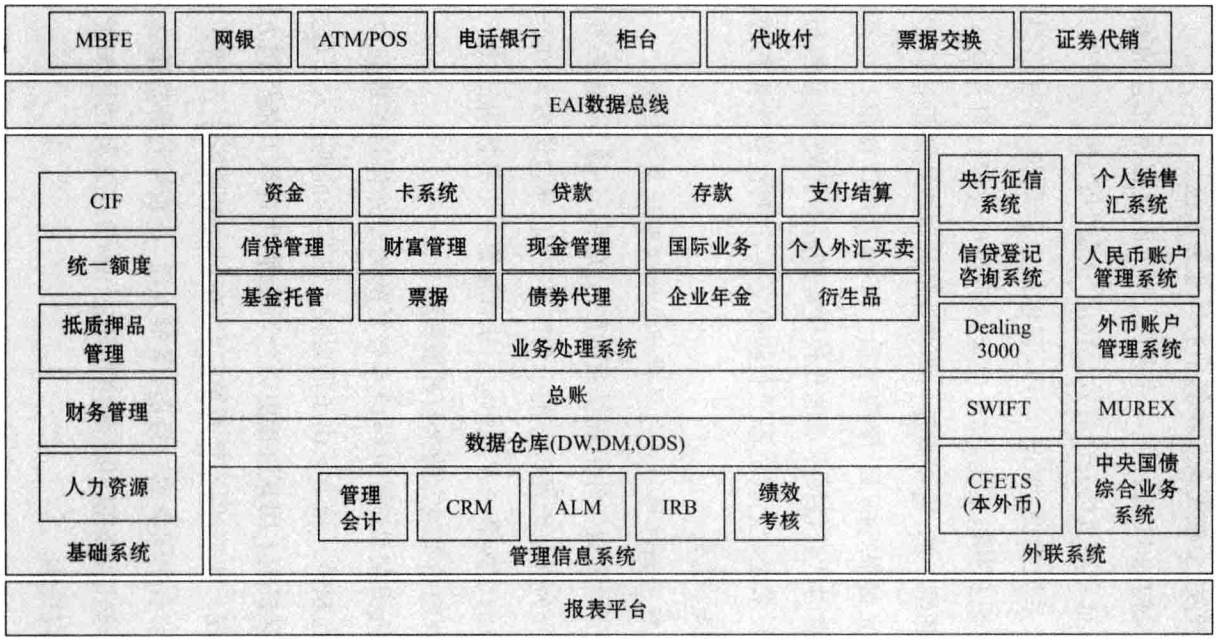
MBFE
网银
ATM/POS
电话银行
柜台
代收付
票据交换
证券代销
EAI数据总线
CIF
统一额度
抵质押品管理
财务管理
人力资源
基础系统
资金
卡系统
贷款
存款
支付结算
信贷管理
财富管理
现金管理
国际业务
个人外汇买卖
基金托管
票据
债券代理
企业年金
衍生品
业务处理系统
总账
数据仓库(DW,DM,ODS)
管理会计
CRM
ALM
IRB
绩效考核
管理信息系统
央行征信系统
个人结售汇系统
信贷登记咨询系统
人民币账户管理系统
Dealing 3000
外币账户管理系统
SWIFT
MUREX
CFETS(本外币)
中央国债综合业务系统
外联系统
报表平台

图 1.1 银行 IT 系统

(2) 外包给发包方合资机构。

金融机构和其他合作伙伴共同设立外包机构，发包方可以按照股权所占百分比对外包机构进行相应的控制。

(3) 外包给直接第三方。

独立第三方作为外包机构，与发包方之间没有任何股权关系，仅仅直接承担外包业务。

(4) 外包给非直接第三方。

金融机构将业务外包给外包提供商，该外包提供商再将这一业务的全部或者部分业务转包给其他外包提供商。

3) 按照供应商的地理分布状况划分

按供应商地理分布状况来划分，可以分为在岸外包和离岸外包。离岸外包是指企业为降低成本、保留核心业务和提高竞争力而将部分业务或流程转移至低成本的国外企业。在岸外包是指发包商和接包商同在一个国家和地区。其中离岸外包又可分为两岸外包和多岸外包，在岸外包包括现场外包和境内外包。

金融 IT 服务外包的意义在于它突破了金融机构用自身资源来塑造竞争力的做法，使他们能有效地运用自身的核心能力去关注战略环节，而把一般性的业务交给外部服务公司去做。因此，外包不是出于单纯节约成本的一时权宜之计，而是金融机构经营的一种战略性措施。金融机构选择适合自身发展需求的合作模式，需要从企业总体战略的制定开始。明确自身未来发展的战略价值定位是什么，对应这些价值定位的核心业务和核心业务环节

是什么，然后确定完成这些核心业务的路径应该如何。在此基础上，外包与否的关键衡量因素一方面在于金融机构的内部因素，尤其是金融机构对于自身核心业务的界定和金融机构自身能力的培养，另一方面取决于外部因素，即服务提供商的服务范围和质量是否能够有效地解决金融机构的担忧和问题。中国金融产业快速发展，外包生态系统也在迅速变化之中，不同的企业会有不同的选择，同一个企业在不同发展阶段也有不同的选择。因此在很长一段时间内多种外包模式将会共存。

1.1.2 国际金融IT服务外包的发展历程和现状

金融信息服务外包始于20世纪70年代的欧美，证券业在低成本的利益驱动下将一些准文书性事务外包。20世纪90年代中后期，在信息技术的推动下，信息技术的应用已不仅仅限于银行的某个部门和环节，而是通过信息技术把整个银行体系整合串联起来，把整个银行的运作实体看作有许多专业化组织共同紧密连接的企业流程运作过程，也就是由组织内的再造提升为组织间的再造。在银行再造(reengineering the bank)的潮流下，欧美的跨国公司如美国运通、GE金融、世界银行、汇丰银行、渣打银行相继在印度、菲律宾等国家建立内包基地，将产品价值链在地理空间上分解外包；1999—2001年，专门承接金融信息业务的专业化企业纷纷建立并造就了一批著名的外包企业，主要是印度公司如Daksh、EXL Service、ICICI One Source，第三方外包出现并发

展；2001—2003年，全球知名金融信息服务商如IBM、埃森哲、HP、EDS等进入印度，以从事软件外包而闻名的Infosys、Satyam建立了专门从事金融信息外包业务的控股公司，外包处于业务流程再造阶段。近年来，随着互联网对金融行业的渗透不断增强，大数据以及云计算概念的流行，金融机构开始与互联网企业等第三方公司合作，不断提供顺应时代发展潮流和客户需求的产品。

目前，国际上包括金融IT服务外包在内的金融信息服务外包的发包方以欧美和日本等发达国家为主，他们凭借自身雄厚的实力和先进的管理，在国际范围内通过把非核心的业务外包给第三方，从而不断降低成本，提高核心竞争力。而印度、中国、菲律宾等发展中国家利用自身的成本和技术优势，把握了金融外包的产业转移潮流，成为金融服务外包的主要接包商。

银行再造是商业银行在信息化浪潮的推动下，寻求银行管理新模式的实践，它起源于20世纪80年代的美国银行界，到90年代已演变成席卷整个西方银行业的一场革命，越来越多的国际型银行走上了银行再造的道路，并取得了巨大的收益。银行再造要求银行放弃过去那种按职能进行分工，然后组合经营的管理办法，借助现代信息技术，重新设计银行管理模式和业务流程，让银行实行科学减肥，使银行集中核心力量，获得可持续竞争的优势。银行再造也可理解为是为了显著地降低成本和提升活动价值而充分依托信息技术和外部专业化组织，以流程系统重新设计为核