商业银行信息科技外包监管研究

汪轶

（西南财经大学中国金融研究中心，成都，610074）

摘要：伴随着银行信息化程度的不断提高，伴随信息科技与银行业务融合度越来越高，信息科技风险事件频繁发生。因此，有必要从信息科技风险的视角对商业银行的监管进行研究。本文在探讨商业银行信息科技外包风险的基础上，结合案例分析和国内外 IT 外包监管比较，指出“从银行监管到服务商监管”是完善我国银行 IT 外包监管的主要方向。

关键词：信息科技风险；外包；服务商监管

引言

信息科技对商业银行的作用和影响是深刻的和全方位的。从信息科技创新的发端起，商业银行就开始接受并逐步大量使用该领域几乎最前沿的技术成果。从最初的单纯的信息传递，到后来对手工劳动的简单替代，直到现在信息科技改变了银行的经营模式、组织结构、决策过程等几乎所有方面。今天的银行，几乎所有的产品、流程、业务活动、风险管理和决策都需要信息科技的支撑，信息科技已经成为现代商业银行正常经营运转的基础设施，其对于商业银行的作用几乎类似于法律对于人类社会的作用。因此信息科技的安全、可靠、有效对整个银行业提高运营效率、加强风险管理具有极其重要意义。但是伴随信息科技在商业银行领域的不断运用，各类风险事件和重大信息科技事故频繁发生，导致商业银行正常经营管理受到重大影响，出现重大损失，甚至引发金融系统性风险。尤其伴随着电子化经营，存款人的财富已经完全电子化，一旦出现系统崩溃，数据无法恢复等重大信息科技风险时，存款人的利益完全得不到保证，整个经济金融系统难以正常运转，甚至整个社会、经济都将出现严重紊乱。

目前信息科技风险监管中的几个重点、难点领域为：信息科技风险计量、信息科技风险评级、外包风险监管和业务连续性风险监管。本文主要讨论的是商业银行信息科技监管中的一个重要领域——IT 外包监管。

一、商业银行 IT 外包理论分析

（一）商业银行 IT 外包的成本收益分析

1.何谓 IT 外包

IT 外包是金融服务外包的形式之一。通常来讲，金融服务外包(Finance Services Outsourcing)是指金融机构将其某一或某一部分事务委托给外部机构或者个人来完成。巴塞尔银行监管委员会公布的《金融服务外包》文件规定，将金融服务外包定义为“受管制实体在连续性的基础上委托第三方来完成一些一般由受管制现在或将来所从事的业务，而不论该第三方当事人是否为某个公司集团内的一个附属机构，或为某个公司集团外的某一当事人”。具体分析来看，金融服务外包不但包括将业务交给外部机构，还包括了将业务交给集团内的其他子公司去完成的情况：不仅包括业务的初始外包，还包括业务的再次外包(也可称之为“分包”)。从外包内容分析来看，金融服务外包包括信息技术外包(即 IT 外包)和金融业务流程外包(BPO) 。

IT 外包，即指金融企业以长时期合同的方式委托信息技术服务商提供某一部分或者全部的信息技术服务，其中主要包括了应用软件开发与服务、嵌入式软件开发与服务，以及其他有关的信息技术服务等方面内容。金融业务流程外包，是指金融企业将非核心业务流程或将某部分核心业务流程转移给承包商来处理，其中主要包括呼叫中心、财务技术支持、消费者支持服务、运营流程外包等内容。

2.IT 外包的动因

（1）提高金融企业核心竞争力

从现有诸多文献来看，核心竞争力理论能够较好的解释客户寻求 IT 外包服务现象。核心竞争力是组织具备的超越具体产品和服务的一种竞争能力，组织的核心竞争力不受单一产业的周期特征约束，能帮助组织适应和及时应对不同的内外部环境。要提高核心竞争力，要求单个组织能在产品开发、业务经营中尽可能做到优势资源集中高效配置，把握重点集中发展其核心业务。对于不同企业而言，都有其自身特点和独特业务。通常，信息技术业务并不是每个企业的核心业务，而通过外包剥离企业的非核心业务，有助把企业集中、合理的配置有限的资源，从而使能使企业有限的技术人员能够更加专注于企业核心业务相关的技术活动，注重企业核心能力的培养及发展，从而实现企业核心竞争力的提高，更好地满足企业长期发展与成长需求，这也是进行信息技术外包的最根本原因[1]。

（2）分流管理和风险压力

有些 IT 项目，比如灾备中心建设，一次性投资巨大，涉及建筑工程、机房配套工程、IT 系统投入、通信网络设备投入等等，后期运营成本高，专业技术及实施难度也非常大，往往与其他建设密不可分，还需要与地方政府、电力和电信等部门合作。如果没有精深的理论作基础和丰富的实际经验作支持，难以进行有效的开发和管理。同时这些投入是为小概率事件准备的，大部分时间处于闲置状态，导致总体投入成本和投资回报率不对称。因此通过外包可以有效的分流自身管理压力。另外，外包服务商可以集中通过保险等形式对 IT 建设项目的风险进行再次转移，有效加长了风险链条，降低了风险集中度，也摊薄了各环节的成本。

（3）控制企业成本支出

多数企业希望利用外包来降低或者至少控制运行成本。相对于企业自身的信息部门，IT 外包商因为具备一定的规模经济效应、专业化服务优势和较强的成本预测能力，因而能够提供相对成本更低、可控性更强的服务。同时利用承包商能够做到现有和未来始终在技术上保持同步优势，具备较高的技术服务水平，企业可以获得低成本接触新技术的机会。这样，借助外包服务降低了财务支出、减少了技术风险的同时，事实上能推动企业的信息技术应用能力。在公司业务增长，不断盈利时可以通过增加外包进一步加强信息科技服务，反之，在业务状况不佳时则可减少外包服务。因此，信息技术外包通过将企业的固定支出变成易于进行调节和控制的可变支出，增强了企业的成本管理能力，有助于降低企业成本支出。转而将这些资源应用于其他更能够盈利的领域，降低企业资金的低效率使用，规避投资的过度分散，确保管理层精力集中在核心业务上。

（二）商业银行 IT 外包的应用分析

1.IT 外包业务的现状

竞争日趋激烈的国内外金融环境使得银行业不断地在挑战中求生存、求发展，由此建立可持续发展的优势地位。但是，随着银行业间的竞争加剧，新业务的层出不穷，银行需要更符合时代的信息系统来满足竞争和业务的需要，这就对银行电子化的建设提出了更加高的要求。银行电子化运作水平作为银行竞争力的重要标志，已经普遍成为银行在市场运作、金融创新、客户服务和量化管理等方面的重要技术基础，直接进入到越来越激烈的银行业市场竞争中。银行信息系统的战略重要性已经得到了广泛的证明和共识。国内外一些银行已经外包出其所有的信息服务职能，而外包部分及全部信息技术活动的趋势也正在日益加剧。

上世纪 90 年代开始，世界各国的银行纷纷采用外包这一金融电子化建设的新战略。美国的摩根大通银行于 2002 年与 IBM 签订了为期 7 年、合同总额为 50 亿美元的 IT 外包服务协议，到目前为止是全球最大的银行 IT 外包项目。由于 IT 的外包，使摩根大通银行全面

[1] 吴卫芬.我国银行业信息技术外包的风险管理研究[M].浙江工商大学硕士学位论文，2008.

提升了核心业务的处理能力，并具备了更好的灵活性和更快的市场反应速度。同时，摩根通过 IT 的外包，又进一步降低了运营成本，使其有更集中的精力去发展核心的金融业务。同年，美洲银行也以 45 亿美元的价格与 EDS 公司签订了为期 10 年的银行 IT 外包服务合同。2002 年，全球又有 5 家较有影响力的银行分别签订了价格在 10 亿美元以上的 IT 外包服务协议，金融业务正在逐步转化为信息管理服务业务。基于巨大的市场竞争压力、客户需求的不断变化和对成本效益的精打细算，都使得各银行不断增加对 IT 系统的投入。

2001 年深圳发展银行与 G D C 公司签订的灾难恢复外包合同，是国内商业银行第一份 I T 大单。2003 年 11 月，光大银行与联想 IT 服务正式签约，联想 IT 服务成为光大银行核心业务和管理会计系统建设及咨询项目的总承包商，合同金额达数千万元；IBM 也获得了招商银行的 IT 外包大单。除了信息系统建设外包，随着一些社会化灾备中心突破性的服务，一些大型金融企业将部分生产中心、甚至是数据中心外包给这些社会化灾备中心，如建设银行等将这类中心建设外包给中金数据系统有限公司。

2.IT 外包业务的趋势与展望

传统外包业务中比较常见的是，信息科技基础设施和运行外包，数据和电信业务外包，应用开发外包，以及应用维保外包。但是近年来外包业务出现了新的发展趋势：一是随着印度、东欧信息科技行业的迅猛发展，离岸外包数量不断增加。离岸外包（off-shore outsourcing）指发包商与接包方来自不同国家，外包工作跨国完成。二是由把服务整体外包给一家供应商，转变为将服务分包给多家供应商；一些技术优势明显的金融机构逐渐成为外包服务供应商，如工商银行即将自行开发的个别系统卖给中国农业发展银行。三是“内包”模式涌现。即机构将其信息科技服务承包给其母公司或所属集团的其他公司。四是业务流程外包数量增加，即将部分业务流程环节分离出来，交给外包服务公司来做，如银行的开户、信用卡申请、支票处理等业务。另外，除了外包业务的大力发展，随着信息技术在商业银行应用范围的不断扩大，与业务融合度不断提高，部分商业银行开始自主承担业务相关软件开发和系统运营等工作。

IT 外包内容的增加，带给银行更多的选择，可操作性也得到增强。信息技术发展迅速，不断有新的技术被开发和应用，为银行信息技术外包提供了更多途径。例如，近年来，炙手可热的“云计算”技术正在被研究用于改善银行业主服务器运算速度问题。尽管出于对“云计算”安全性等问题的不同考虑，国内金融机构仍停留在观望阶段，不敢贸然使用“云计算”，但这并不意味着“云计算”在我国金融行业没有生存发展空间。根据媒体报道，中国惠普公司正针对金融机构对“云计算”安全性能担忧的问题，进行大规模软件开发测试，旨在满足质量管理需求，开拓信息技术外包新模式。

（三）商业银行 IT 外包风险理论剖析

IT 外包可能为企业降低成本，集中精力专注于核心业务，提高企业核心竞争力，但同时也为企业带来了新的金融风险。Lacity 和 Hirschheim (1993)通过对财富 500 强中 14 家企业 IT 外包实践进行研究发现，IT 外包并不完全如理想中那样完美，外包供应商并非企业的战略伙伴，其效率并非最优，甚至并不完全具备成本优势。这项研究给当时很多热衷于外包的企业敲响警钟，也为 IT 外包风险研究开启了先河。当前，IT 外包面临的主要风险有：

一是核心技术受制于人的风险。由于外包，使得银行不再需要对 IT 系统进行开发和维护，也不需要对 IT 资源进行控制和管理，因此将放松自身对信息科技的管理，难以全面认识新的 IT 知识。并且，在外包过程中，往往过于依赖外包服务商的力量，使得核心技术被人钳制，从而可能失去对各类 IT 资源进行客观评估的业务能力，很难再借助引入新 IT 技术来开拓自身业务。

二是 IT 资源支离破碎的风险。银行如果将与业务关系密切的 IT 资源部分外包或者分别外包，就有可能出现协调困难。如某银行将部分业务分别外包给计算机服务商和电信运营

商，一旦出现系统响应迟缓等问题，计算机服务商可能将原因归于运行线路状况问题，而电信运营商则会认为是计算机服务商的设备故障。双方的争执与推诿，往往会掩盖问题的真相，给银行带来损失。

三是信息科技资源与核心业务不匹配的风险。银行与外包服务商的关注点不同，银行更为关注信息科技资源在关键点上能为业务、经营发展提供支持，但服务商则更为关心如何有效的开发信息科技系统，而忽视为什么要开发这个系统，因此开发出的系统可能在技术上具有更具备优势，但在与银行核心业务的有效衔接上则存在一定的问题[2]。

四是商业合作的不确定性风险。由于外部多变的商业环境，可能会导致发包商在原有外包合同签订后，提出新的合作要求。通常，这种情况是难以避免的。不过，改变业务合作并不总会导致商业损失，业务合作中良好的发包企业-服务商关系有助于双方能够建设性地应对和处理各类新问题。

五是隐性成本支出风险。主要包括：在选择服务商、进行业务剥离时的交易成本、转换成本、服务商要求的额外费用等；最为严重并不可估量的成本支出是： IT 设施运行质量不达标，以及由此产生的系统故障，乃至业务停顿等重大损失。

（四）商业银行 IT 外包风险与其他信息科技风险关联性研究

银行 IT 外包风险可以说是信息科技风险中的核心风险，与其他类风险休憩相关，突出表现在 IT 外包风险将引发两类重要风险：一是由于服务商在技术、操作方面出现故障或者业务中断从而可能危及银行的业务开展的连续性；二是由于服务商在技术、操作方面出现故障或者受到外来攻击而可能危及银行系统的信息安全。Aubert (1998)等人在研究 IT 外包的风险问题时指出，发包企业面临的风险有委托人（发包企业）、代理人（服务商）和交易等三个方面的来源，本文依此思路对银行 IT 外包风险进行了关联性分析。来源于发包银行的风险有四种：IT 资源变得支离破碎、了解不到新的 IT 知识、缺乏创新能力及 IT 资源不再与核心业务休戚相关，由此导致银行面临信息科技基础设施建设风险和业务连续性风险。来源于服务商的风险有五种：服务人员缺乏业务经验、服务商缺乏符合市场的新技术、隐藏的成本、与服务商相关的业务连续性风险及与服务商有关的信息安全风险。来源于交易的风险有三种：服务商、发包企业管理者与技术人员之间可能缺乏沟通、商业上的不确定因素及削弱对 IT 的管理，同样可能导致业务连续性风险和信息安全风险。

[2] 梁贵民，曹晓军.我国银行业信息技术外包的风险管理研究[J].现代商业银行.2002(9)：32.

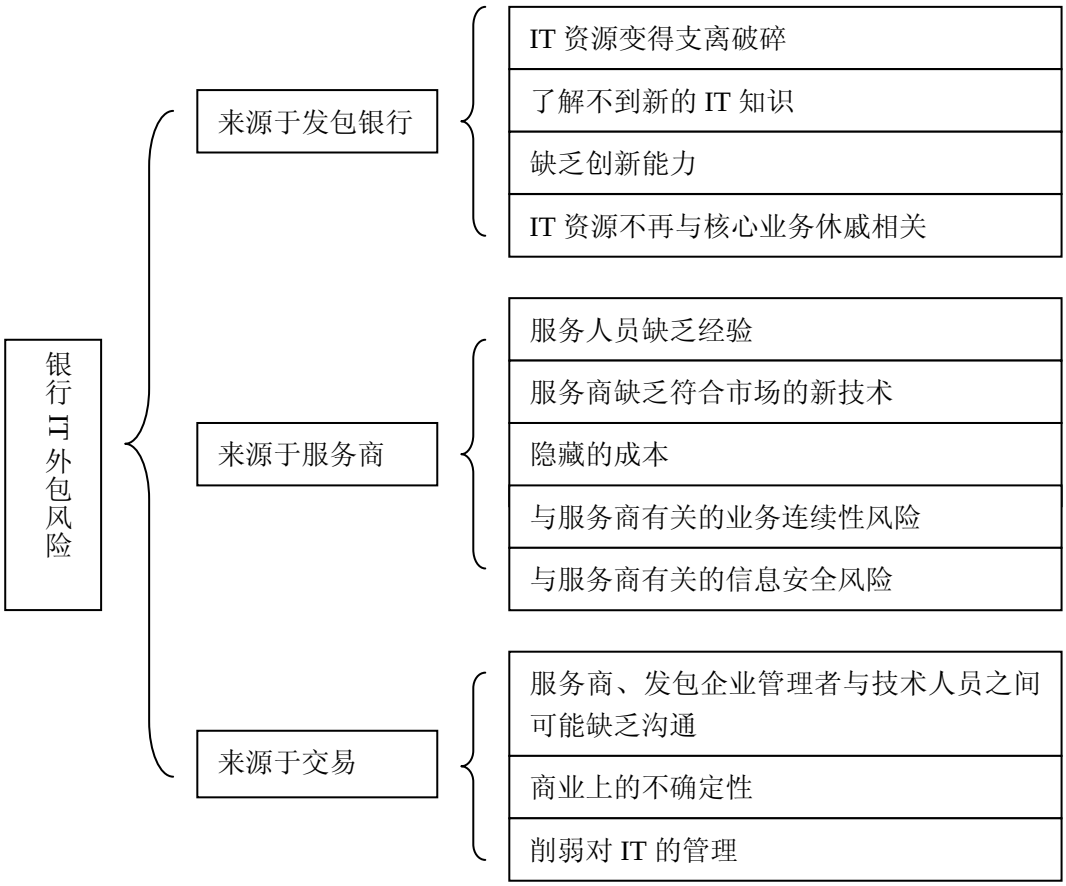

图 1　银行 IT 风险分类

二、商业银行 IT 外包风险案例分析

（一）XX 银行外包业务管理现状案例

XX 银行是国内一家大型上市银行，但是其外包业务管理上，首先没有明确的技术外包策略，没有统一的技术外包服务商市场准入标准，对外包服务商资质、专业能力缺乏必要的审核和评估；对外包服务商技术实力、经营状况、社会信誉等因素没有进行综合评定，对其服务水平缺乏评价考核机制。其次，未对外包产生的风险迁移情况进行分析。在开发测试、运行维护等各项外包工作中缺乏针对外包商突然离场的应对措施。第三，缺乏对外包人员有效管理。外包人员访问本行计算机资源的身份认证工作有漏洞，对离职外包人员未及时调整访问权限。外包人员可随意携带笔记本电脑、3G 网卡、移动存储介质等设备进出机房，甚至清洁工自行保管 2 张可 24 小时进入机房各区域的门禁卡，且长期有效。

（二）客户信息资料被窃取案例

2009 年，XX 银行发生一起科技外包人员窃取银行客户信息，伪造银行卡，在 ATM 机上盗取持卡人资金的案件。事情经过是：XX 行与 XX 公司签订开发合同，开发银行 ATM 机监控软件，同时约定该软件由 XX 公司进行维护。2009 年，维护人员上门维护 ATM 机监控系统，通过终端机将服务器有关客户数据库设置为共享状态，在终端机上操作数据库，插上 U 盘，拷取数据库中客户信息数据，拷出的数据库字段主要为“卡号、卡有效期、CVV 等”。其中 CVV 为磁条安全验证码，是制卡的关键性安全认证标志。拷出的数据库记录经估算约十几万条。利用窃取的信息伪造银行卡，通过猜测银行卡密码，在 ATM 机上窃取持卡人资金，窃取人民币数十万元。案件主要原因：外包合同从未包含涉及数据信息安全保密的条款，也未单独签订安全保密协议。

（三）核心系统瘫痪案例

XX 银行核心系统长期以来一直依靠外包服务商进行开发。现正在使用的系统设计时最大日均处理能力为 80 万笔，但随着业务的发展，现日均处理能力要求达到 210 万笔，导致该行系统处理能力与系统负载之间缺口极大。而外包服务商已不再对该核心系统提供升级服务，并且该行自 2009 年起，没有购买维保服务。2010 年，终于由于数据库“长事务”引发逻辑故障，导致业务中断。而由于该行的技术人员不掌握该系统的核心技术，加之对外包服务商缺乏有效的管理，导致系统维修不及时，致使业务中断时间长达 4 小时 20 分钟，在全国引发了极大的声誉风险。

三、国内外银行 IT 外包监管比较研究

（一）巴塞尔银行监管委员会《金融服务外包》文件

巴塞尔银行监管委员会、证券交易委员会国际组织、国际保险监督官协会三方于 2004 年 8 月举办联合论坛，成立联合工作组，并发布《金融服务外包征求意见稿》,《意见稿》对金融服务外包管理的指导原则做出了明确规定，并指出了金融外包的特殊性，对金融机构开展外包活动具有重大指导意义[3]。其中指导原则共有 4 条，分别对从事外包活动的金融机构和监管当局的权利、责任做出相应的规定，以尽可能的降低实施外包活动带来的风险。2005 年 2 月，联合论坛正式出台《金融服务外包文件》。

《金融服务外包文件》明确了具体指导原则，其中涉及到对金融机构责任、义务进行规范的内容主要包括：金融机构需要制定综合政策，评估拟外包的业务、系统是否适合进行外包，在充分评估的基础上，进行外包决策；董事会应对制定外包政策、执行外包政策以及所有相关事项负责；金融机构应制定全面的外包风险管理计划，以处理外包事务及与外包商的关系；金融机构不得利用外包减少自己应该对各相关方承担的责任，即包括对客户的责任，也包括对监管当局的责任；金融机构在选择外包服务商时，应做到尽职调查，明确外包商应该承担的责任、履行的义务，以及通过外包要实现的目标，并将条款细化体现在书面合同中；金融机构与外包服务商都应该制定相应的应急预案，主要包括危机恢复方案、定期对后备设施进行检测安排等内容；金融机构应采取有效的措施，要求外包商保护本机构及其客户的保密信息不被泄露，外包商不能有意或无意地向没有授权的第三方披露任何信息。涉及到对监管当局责任进行规定的内容主要有：监管当局应将外包纳入对金融机构持续性评估的环节。同时，监管当局应采取有效手段防止金融机构利用外包逃避有关监管要求；监管当局还应该清醒的认识到，如果多家金融机构的外包业务过于集中在有限的几个外包服务商时，将产生集中性风险。

（二）发达国家银行 IT 外包监管

1.美国

随着外包服务业的迅速发展，美国银行业的技术服务外包已经相当普遍，数据中心、灾备中心、信用卡、ATM 设备等都可以外包给第三方技术服务提供商（Technology Service Provider,简称 TSP）。

针对这种情况，美国各个监管当局出台了一系列指引、办法，对银行业务、技术、系统、服务外包业务、以及银行在各种外包关系中应该承担的风险管理责任等进行明确规定。有关监管法规、指引主要包括：FFIEC 的《技术服务外包风险管理指引》(2000 年 11 月)；OCC 公告 2001-47 号,《第三方关系：风险管理原则》(2001 年 11 月);《选择外包商的有效办法》、《对技术外包商操作风险的管理工具:服务水平协议》、《管理多方外包商的技术》(联邦存款保险公司，2001 年 6 月);《技术服务商监管手册》、新版的《FFIEC 技术服务外包 IT 检查手册》（2004 年）。

[3] Basel Committee on Banking Surpervision.Outsourcing in financial Services, Feb 2005.

根据美国银行服务公司法案（Bank Service Company Act）要求，美国的银行监管机构对于为银行提供服务的 TSP 具同等的监管权力。由于外包业的不断发展也使得 TSP 成为美国银行监管的对象，尤其是一些大型 TSP 同时为多达几十家乃至上百家银行金融机构提供服务，那么相应的技术风险也就集中到这些技术服务提供商，迫使美国监管机构不断加强对 TSP 的监管。“服务外包，责任不外包”是美国监管机构的一个重要监管理念，即金融机构可将服务外包给 TSP，但风险管理的责任依旧由金融机构自身承担。在对金融机构的监督检查中，监管者要重点检查其选择 TSP 的流程、与 TSP 签署的协议、外包项目的管理等等多方面内容，以确保银行在使用 TSP 的过程中有效地落实了风险控制相关措施。

由于一个 TSP 可为多家银行金融机构服务，但这些银行机构可能隶属于不同的监管机构，如何划分对 TSP 的监管职责，对于如何避免重复监管，曾一度困扰有关的监管机构。美国各监管机构在 FFIEC 的协调下，对多家机构都具有监管职责的 TSP 采取了“轮流主持”的方法，即每隔两年，明确一个主监管机构，称作 Agency in Charge，在这两年内的监管则由该机构主导，其余机构可以参与配合，主监管机构的监管报告与其他有关机构进行共享，避免了重复监管的问题。随着 TSP 不断壮大，出现了大型的 TSP，即 MDPS,目前美国有 25 家，对 MDPS 的监管由 FFIEC 直接负责监管。

2.其它国家

英国、日本等西方国家也在 2000 年后发布了银行 IT 外包监管指引（表 8-1）。

表 1　各国 IT 外包监管指引

国家	时间	监管指引
英国	2004 年 12 月	金融服务管理局提出了对银行外包事项的新的指引，建议银行金融机构应设立必要的外包程序
日本	2001 年 4 月	日本银行发布金融机构稳健运行文件，金融服务局发布金融机构检查指南，提出了外包业务风险管理的规范意见，并明确了检查内容
瑞士	1999 年 8 月	瑞士联邦银行委员会出台《银行和证券公司外包指引》
澳大利亚	2002 年 7 月	发布并实施关于银行外包业务的“审慎标准”
加拿大	2001 年 5 月	金融机构监督办公室发布外包业务规范指导方针

（三）我国银行 IT 外包监管

银监会《商业银行信息科技风险管理指引》专门用一章篇幅阐述了外包问题，而且强调了商业银行在外包业务执行过程中的风险管理职责。

表 2　《商业银行信息科技风险管理指引》对外包的规定

条文	内容节录
第五十五条	商业银行不得将其信息科技管理责任外包，应合理谨慎监督外包职能的履行
第五十六条	商业银行实施重要外包（如数据中心和信息科技基础设施等)应格外谨慎，在准备实施重要外包时应以书面材料正式报告银监会或其派出机构
第五十七条	商业银行在签署外包协议或对外包协议进行重大变更前，应做好相关准备
第五十八条	商业银行在与外包服务商合同谈判过程中，应考虑多种因素
第五十九条	商业银行在实施双方关系管理，以及起草服务水平协议时，应考虑多种因素
第六十条	商业银行应加强信息科技相关外包管理工作，确保商业银行的客户资料等敏感信息的安全
第六十一条	商业银行应建立恰当的应急措施，应对外包服务商在服务中可能出现的重大缺失。尤其需要考虑外包服务商的重大资源损失，重大财务损失和重要人员的变动，以及外包协议的意外终止
第六十二条	商业银行所有信息科技外包合同应由信息科技风险管理部门、法律部门和信

	息科技管理委员会审核通过。商业银行应设立流程定期审阅和修订服务水平协议

四、IT 外包监管理念重构——从银行监管到服务商监管

银行 IT 外包业务风险既来源于发包银行企业和交易过程，也来源于信息技术服务商（TSP），但有时来源于 TSP 的风险，往往超出了银行的控制范围，即使银行严格落实了风险管理职责，TSP 风险有时也很难有效防控，因此由监管者出面监管 TSP 风险是银行 IT 外包监管的重要组成内容。我国目前对银行 IT 外包的监管强调了银行的风险管理职责，但尚未对 TSP 纳入直接监管对象，借鉴发达国家，特别是美国的经验，笔者认为应将 TSP 监管归入 IT 外包业务监管体系之中，并作为完善我国银行 IT 外包业务监管的主要方向。本文对国内开展 TSP 监管的模式和检查程序进行了设计。

（一）服务商风险评估与管理

1.确定 TSP 监管基本方案

TSP 监管方案应包括：①确定当前的、潜在的、可能引起 TSP 对金融机构提供服务不利因素的风险。②分析评估 TSP 风险管理及控制措施的完整性以及有效性。③建立 TSP 对金融机构进行服务遵守相应法律法规的承诺。④及时、明确地将沟通结论、相关建议及任何需整改的内容反馈到 TSP 管理层。如有必要的话，可反馈给 TSP 所服务的金融机构以及其他监管部门。⑤获得 TSP 关于改进巨大缺陷的承诺，并跟踪、验证其改进的效果。⑥监测 TSP 产品、服务或者风险管理的重大改变（可能造成服务金融机构不利影响的改变）。

2. TSP 风险评估

交易风险（即业务操作风险）是与 TSP 有关的，是数据处理过程中最主要的风险，可以是由于欺诈，错误，无法提供产品服务、保持竞争地位或管理信息而引发的。它存在于 TSP 每一个产品或服务传送中，不仅包括了操作和交易风险，也包括客户服务领域、系统开发支持、内部控制程序和业务量等诸多方面的风险。

TSP 交易和操作的风险数量是其已存在的风险水平，检查者在分析评估 TSP 交易/操作风险时应当考虑以下内容：①TSP 的财政状况。②合计服务金融机构的客户数量。③合计服务金融机构的业务量、货币量。④合计服务受监管金融机构的业务量、货币量。⑤提供产品线的数量和形式。⑥所应用技术的可靠性。⑦业务持续性规划的可靠性。

交易和操作风险管理的效果，取决于有多好的识别、计量、控制、监测风险，监管者在分析评估 TSP 交易操作风险质量时还应该考虑以下内容：①TSP 政策的质量。②控制和操作过程的完善性。③技术和管理的专业程度。④TSP 管理层失察。

交易风险同时也可能会导致其他风险，例如信贷利率价格，合规性，流动性，战略以及声誉风险。与 TSP 有关的风险具体如下：①声誉风险——信息技术错误，延误，遗漏等情况公开到市场上，或者直接对其所服务的银行产生重大影响。例如，一家 TSP 服务商未对业务关键环节制定完善的业务恢复预案，极有可能损害其负责的金融机构对客户提供重要服务。②战略风险——-TSP 提供的信息不准确时，会误导其所服务的金融机构制定低质量的战略决策。③合规性风险——向消费者披露不正确或时间错位的信息，或者未经授权披露客户保密信息，涉及到的金融机构可能面临民事诉讼或金钱处罚。例如，TSP 经常同意保持与银行法规相一致来执行信息披露要求，但一旦他们未及时跟踪法规变化时，会导致其服务的金融机构合规风险增加。④信贷利率价格风险——数据处理失误会导致其所服务的金融机构信贷利率价格风险增加，主要体现在金融机构投资收益及回报预期上。

3. TSP 风险管理

监管者应当意识到，管理规范，特别是涉及到风险管理时，各金融机构和 TSP 都有所不同，取决于其各自业务的规模、性质、复杂性及风险水平。因此，监管者也应注意到，若

机构信息系统环境不太复杂，那么高级的详细的格式化系统和控制措施可能不需要。

金融机构在选择 TSP 时应该对其进行全面的调查，包括确认 TPS 自身使用的风险管理系统，金融信息安全状况，确保其具备充分的自身安全保密措施。金融机构还应该跟踪 TPS 的服务水平报告、审计、内控测试结果以及其他的 TSP 分析评估报告。监管者在确认 TPS 薄弱的管理控制措施后，可要求其进行改进，在这种情况下，TSP 服务的机构需要采用补救措施，毕竟金融机构承担着其风险管理的最终责任。

周密合理的审计体系是强大风险管理和有效内控的必备条件。完善的内外部审计体系则能有效地防止欺诈，并能为董事会提供出色的内控措施的重要信息。监管者应当鼓励使用以风险为立足点的审计体系，机构董事会，管理层和审计人员能够以此作为支撑，将有效的风险管理资源，集中使用在风险最大的领域。此外，完善的审计和内控体系能协助监管者有效使用监管资源，制定现在及未来的监管工作要点，并以此作为评估机构风险管理质量的依据。若一个 TSP 有完善的风险审计体系，一般来讲需要较少的外部检查。

（二）服务商监管内容与标准

1. 监管频率

监管频率是按照各 TSP 不同的风险状况决定的，检查人员则根据风险评估来确定监管检查频率。有时，检查者也会根据当时的重点内容，按照一些正常安排之外的检查。正常情况下，服务超过一种类型金融机构的 TSP，必须与监管机构协调，确定会面时间，并根据 TSP 服务内容和范围，采取与地区监管局或监管小组委员会会面的形式。

2. 监管责任

监管者对信息技术检查的管理和综合表现负责，这些责任包含但不限于：①发展、维持风险检查策略及检查范围的有效性。②与各有关的监管部门做好沟通工作，包括检查方案，当面会议，以及书面交流形式。③协调检查时间。④在现场检查前，通过非现场检查与 TSP 沟通协调好现场检查内容。⑤监督检查队伍，确定打分、检查结论、操作、工作记录、以及工作日期与赋予的监管策略相一致。⑥检查完成后与被检查者管理层和董事会会面（“退出会议”），如有必要，会上对其通报检查结论以及后续跟踪建议等内容。⑦书写检查报告。

3. 监管方案

检查方案是有效监管的必要组成原素，帮助检查者发展风险策略及检查 TSP 工作的有效性。它始于检查者对现有及预期风险的评估，应当特别关注兼并和收购，新产品、提供服务或管理的变化。监管者在现场检查前必须首先收集、整理、分析有关信息内容，其他检查准备工作取决于 TSP 结构的复杂性以及所提供服务的种类。信息来源包括但不限于：①核准的监管策略。②此前的检查报告，工作记录，及相关建议。③监管行动和信件。④如可能的话，内外部审计报告。⑤内部风险评估或其他审查，其中包括安全性测试。⑥与 TSP 有关的临时信函或者备忘录。⑦财务报表和股票研究报告。⑧新闻媒体报道。⑨可能的话，TSP 的官方网站。⑩相关上市公司有关信息。

4. 监管范围

监管者应该事先确定检查范围和计划完成的时间。对于不只一个数据处理中心的 TSP，监管者应当分析其分支数据处理中心的相关风险，检查范围应包含数据处理总部及任何检查计划中的分支机构，并在备忘录里特别列举上次检查中存在风险较大的分支机构、将来要检查的区域及检查安排的相关信息。备忘录也应该列举检查的目的、任务、工作预算，以及其他有关信息。在确定检查范围的时候，监管者应该与他们的上级监管层保持沟通，必要时，也与其他相关机构做好沟通工作。如果检查范围、参与人员，预计检查时间发生较大变化，EIC 应当及时与其上级及检查小组进行沟通。

5.通知义务

至少在四周前，EIC 应该和 TSP 联系，通知他们将要开展的检查工作，并要求其在检

查到来前做好有关的准备工作。

6.“进入会议”

监管者应安排一次检查前的会议(“进入会议”),向 TSP 的核心管理层面介绍检查队伍、明确各检查区域的主要联络人员。此会议程至少还包含以下内容:①对管理和审计的巨大关注度。②计划或已开始的重大硬软件研发情况。③自上一次检查后的进展情况(例如,企业控制和管理上的变化)。④上次检查和审计报告上列举问题采取的相应措施。⑤财务表现。⑥在经营、战略、提供服务及客户基础方面的重大变化情况。⑦经济和市场方面的竞争条件。⑧与管理层或审计就检查情况通报的相关会面计划。⑨TSP 与客户之间的标准合同规定 。

7. 工作文件

工作文件是用来记录检查过程从而得出检查结论,需要在任何领域,做好充分的准备,好让阅读者以此明白检查了什么,为什么做了这些检查,以及得出检查结论的依据是什么。工作文件应不仅包含必要的相关信息,如支撑检查结论的依据,违法的相关法律法规,以及任何需要改进的措施,而且必须根据检查结论清楚地列示 TSP 需要后续进行的工作。所有的结论必须准确的记录,并保存在工作文件中,检查者可随时以通过调查、观察、询问、确认、以及分析测试等手段获取检查证据。EIC 在离开前,需要对所有工作文件进行复核,确保工作文件的总体质量符合会员机构的有关标准,并承担相应责任。工作文件是检查报告中的一个组成内容,检查者必须任何时间保证其安全性。在没有授权的情况下,检查者在 FFIEC 机构外不可以将文件脱手。检查者及有关人员必须保证所有与检查相关敏感信息在其笔记本电脑中的安全、可靠,检查完全结束后,检查者和相关人员必须立刻清除。如工作文件以电子文档的形式保存,授权员工在共享时必须通过安全的传输途径,避免信息被未授权者非法获取。

8.“退出会议”

“退出会议”目的就是将检查发现、结论、以及相关建议及时通报至 TSP 高管层,并获取他们有关改进行动的承诺。监管者应具体负责安排会议及会议议程,议程应该包括一份草拟的、包含主要问题的检查报告,所有出席者应在几个工作日前被告知会议的具体时间和地址。 “退出会议”前,监管者应该将所有的检查结论及有关建议通报给 TSP 中、低级管理层,应该对检查结论中任何有异议的内容进行研究,并在“退出会议”前再次确认检查事实,补充相应证明材料。

参考文献

[1] Aubert, B. A., Patry, M., Rivard, S. Assessing the Risk of IT Outsourcing[C]. Proceedings of the 31st Hawaii International Conference on System Sciences, Hawaii. CIRANO, 1998

[2] Ahmad Abu-Musa， Exploring the importance and implementation of COB1Tprocesses in Saudi organizations[J], Information Management&Computer Security Val. 17 No. 2, 2009，P73-95

[3] APRA，2006，Prudential Standard APS 231 outsourcing

[4] Basel Committee on Banking Surpervision.Outsourcing in financial Services, Feb 2005.

[5] Brian Cleary，How Safty is Your Data?[J] STRATEGIC FINANCE，October2008 P33-37

[6] Basel Committee on Banking Surpervision. Electronic Banking Risk Management Issues for Bank Supervisors, Electronic Banking Group Initiatives and White Papers, Oct 2000

[7] Benoit A Aubert,Suzame Rivard,Michel Patry. A transaction cost model of IT outsourcing, Information & Manangement,2003

[8] Earl, M. J. The Risks of Outsourcing IT[J]. Sloan Management Review, 1996, 37(3): 26-32

[9] FDIC，2006，Guidance for Financial Institutions on the Use of Foreign-Based Third-Party Service Providers

[10] Huff, S. L. Outsourcing of information services[J]. Business Quarterly, 1991: 62-65

[11] Jurison, J. The role of risk and return in information technology outsourcing decisions[J]. Journal of Information Technology, 1995, 10: 239-247
[12] Pinnington, A., Woolcock, P. How far is IS/IT outsourcing enabling new organizational structure and competences?[J]. International Journal of Information Management, 1995, 15(5): 353-365.
[13] Sineenad Paisittanand a. David L. Olson.A simulation study of IT outsourcingin the credit card business, European Journal of Operational Research 175 (2006)，P1248-1261
[14] 吴卫芬.我国银行业信息技术外包的风险管理研究[D].浙江工商大学硕士学位论文，2008.
[15] 梁贵民,曹晓军.我国银行业信息技术外包的风险管理研究[J].现代商业银行.2002(9)：32.
[16] 季冬生.信息技术与金融发展[M].北京：中国金融出版社，2004.
[17] 王漩,李毅.金融监管理论演化进程及其趋势[J].华南金融研究，2001(6):8-10.
[18] 裴桂芬.银行监管的理论与模式[M].北京：商务印书馆，2005.
[19] 胡维波.金融监管的理论综述[J].当代财经，2004(3):50-53.
[20] 白宏宇.百年来的金融监管：理论演化、实践变迁及前景展望[J].国际金融研究，2000(1):35-41.
[21] 李东荣.我国金融业信息化建设的成就与发展思路[J].中国金融.2009(18)：14-16.
[22] 杨涛.商业银行信息科技风险量化与管理研究[J].信息安全与技术.2010(8)：66-70.
[23] 张倩,张云志,祁妙.关于商业银行信息科技风险的调查与思考[J].中国信用卡.2009(2)：16-20.
[24] 王忠生.我国金融监管制度变迁研究[D].湖南大学博士论文，2008.
[25] 陈文雄.信息科技风险监管和管理[J].金融电子化，2009（10）：27-29.
[26] 银监会.商业银行操作风险资本计量指引，2008.
[27] 公安部网络安全监察局.信息网络安全与病毒疫情调查分析报告，2010.
[28] 龙江涛,李新春,古凤.我国网络银行风险及对策研究[J].金融与经济.2008(4):90-91.
[29] 贺建华.网上银行安全策略.计算机世界报[N].2001(3).
[30] 满海红.金融监管理论研究[D].辽宁大学博士论文，2008.

A Study on the Regulation of Commercial Banks' Information Technology Outsourcing

Wang Yi
（Chinese Financial Research Centre of Southwestern University of Finance and Economics,Chengdu,610074）

Abstract: With the increasing application of IT system, and along with the coherence between information technology and bank business which is getting higher and higher, IT risk events happen frequently. Therefore，it' s necessary to study the commercial bank regulation from the perspective of IT risk. On the basis of exploring the risk of commercial banks' IT outsourcing, and combining international practices on IT outsourcing supervision, the thesis suggests that extending supervision from banks to cover IT service provider is the main direction.
Keywords: information technology risk; outsourcing; service provider regulation

收稿日期：2011-07-09
作者简介：汪轶，西南财经大学中国金融研究中心金融学博士，研究方向：金融理论与实践