中国银监会关于印发银行业金融机构信息科技外包风险监管指引的通知

各银监局、各政策性银行、国有商业银行、股份制商业银行、金融资产管理公司，邮储银行，各省级农村信用联社，银监会直接监管的信托公司、企业集团财务公司、金融租赁公司：

现将《银行业金融机构信息科技外包风险监管指引》印发给你们，请遵照执行。

2013 年 2 月 16 日

银行业金融机构信息科技外包风险监管指引

第一章　总则

第一条　为规范银行业金融机构的信息科技外包活动，降低信息科技外包风险，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》等法律法规，制定本指引。

第二条　在中华人民共和国境内设立的政策性银行、商业银行、农村合作银行、省（自治区）农村信用社联合社适用本指引。银监会监管的其他金融机构参照本指引执行。

第三条　本指引所称信息科技外包是指银行业金融机构将原本由自身负责处理的信息科技活动委托给服务提供商进行处

理的行为，包含项目外包、人力资源外包等形式。原则上包括以下类型：

（一） 研发咨询类外包：科技管理及科技治理等咨询设计外包，规划、需求、系统开发、测试外包；

（二） 系统运行维护类外包：包括数据中心（灾备中心）、机房配套设施、网络、系统的运维外包，自助设备、POS 机等远程终端及办公设备的运维外包；

（三） 业务外包中的信息科技活动：市场拓展、业务操作、企业管理、资产处置等外包中的系统开发、运行维护和数据处理活动。

第四条 本指引所称关联外包是指服务提供商为银行业金融机构的母公司或其所属集团子公司、关联公司或附属机构提供信息科技外包。

第五条 信息科技外包可能产生如下风险，并导致银行业金融机构的战略、声誉、合规风险：

（一） 科技能力丧失：银行业金融机构过度依赖外部资源导致失去科技控制及创新能力，影响业务创新与发展；

（二） 业务中断：支持业务运营的外包服务无法持续提供导致业务中断；

（三） 信息泄露：包含客户信息在内的银行业金融机构非公开数据被服务提供商非法获得或泄露；

（四） 服务水平下降：由于外包服务质量问题或内外部协作效率低下，使得银行业金融机构信息科技服务水平下降。

第六条 本指引所称机构集中度风险是指银行业金融机构将信息科技外包服务集中交由少量服务提供商承接而产生的风险，该风险可能造成集中性的服务中断、质量下降、安全事件等。

第七条 本指引所称同业托管机构是指作为外包服务提供商为其他同行业金融机构提供信息科技外包服务的银行业金融机构。

第八条 银行业金融机构应当将信息科技外包管理纳入全面风险管理体系，建立与本机构信息科技战略目标相适应的外包管理体系，控制或降低由于外包而引发的风险。

第九条 银行业金融机构应当建立信息科技外包管理组织架构，制定外包管理战略，定期进行外包风险评估，通过服务提供商准入、评价、退出等手段建立及维护符合自身战略目标的供应商关系管理策略。

第十条 银行业金融机构在实施信息科技外包时应当坚持以下原则：

（一） 以不妨碍核心能力建设、积极掌握关键技术为导向；

（二） 保持外包风险、成本和效益的平衡；

（三） 强调外包风险的事前控制，保持管控力度；

（四） 根据外包管理及技术发展趋势，持续改进外包策略和措施。

第十一条 银行业金融机构在实施信息科技外包时，不得将信息科技管理责任外包。

第十二条 对于不涉及银行客户及内部信息转移的信息

科技产品采购、维保，及通讯线路租用、支付或清算系统接入等信息科技公共基础设施服务，银行业金融机构应当充分评估其信息科技风险，按照本指引第五章要求进行管理。

第二章　外包管理组织架构

第十三条　银行业金融机构董事会及高级管理层应当严格落实信息科技外包风险管理的相关职责，明确信息科技外包风险管理的主管部门，制定并审批信息科技外包战略，审议信息科技外包管理流程及制度，督促并监控信息科技外包风险管理效果。

第十四条　信息科技外包风险主管部门的主要职责包括：

（一）　对外包风险进行识别、评估与风险提示；

（二）　监督、评价外包管理工作，并督促外包风险管理的持续改善；

（三）　向高级管理层定期汇报信息科技外包活动相关风险管理情况；

（四）　董事会或高级管理层确定的其他信息科技外包风险管理职责。

第十五条　银行业金融机构应当在信息科技管理部门或信息科技外包活动执行部门内建立信息科技外包管理执行团队，并配备足够人员履行以下职责：

（一）　实施信息科技外包战略；

（二）　制定并执行信息科技外包管理制度与流程；

（三） 执行供应商准入、评价、退出管理，建立并维护供应商关系管理策略；

（四） 制定保障外包服务持续性的应急管理方案，并组织实施定期演练；

（五） 对外包过程中的各项管理活动进行监控及分析，定期向信息科技及外包风险管理主管部门报告外包活动情况。

第三章 信息科技外包战略及风险管理

第一节 信息科技外包战略

第十六条 银行业金融机构应当以提升信息科技队伍能力，提高科技管理及创新水平，掌握信息科技核心技能为目标，基于信息科技战略、外包市场环境、自身风险控制能力和风险偏好制定信息科技外包战略，包括：不能外包的职能、资源能力建设方案、供应商关系管理策略和外包分级管理策略。

第十七条 银行业金融机构应当根据自身信息科技战略明确不能外包的职能。涉及战略管理、风险管理、内部审计及其他有关信息科技核心竞争力的职能不得外包。

第十八条 银行业金融机构应当根据外包战略制定资源、能力建设方案，通过补充人员、提升技能、知识转移等方式，有针对性地获取或提升管理及技术能力，降低对服务提供商的依赖。

第十九条 银行业金融机构应当建立与自身规模、市场

地位相适应的供应商关系管理策略。通过准入和退出机制合理管控各类高风险服务提供商的数量，实现以下目标：防范行业垄断和机构集中度风险，通过引入适当的竞争在降低采购成本的同时提高服务质量，合理管控服务提供商的数量从而降低风险及管理成本等。

第二十条 银行业金融机构可以按照外包服务性质和重要性程度对服务提供商进行分级管理，对不同级别的服务提供商采取差异化的管控措施，在有效管理重要风险的前提下降低管理成本。

第二十一条 银行业金融机构要同母公司或集团公司协同做好外包服务及服务提供商的管理工作，但应当保持关联外包有关决策的独立性，避免因关联关系而降低外包活动的风险控制水平。

第二节 信息科技外包风险管理

第二十二条 银行业金融机构信息科技外包风险管理部门应当至少每年开展一次全面的外包风险管理评估，保持评估的独立性，并向高级管理层提交评估报告。评估内容包括：信息科技外包战略执行情况、外包信息安全、机构集中度、服务连续性、服务质量、政策及市场变化对外包服务的影响分析等。

第二十三条 银行业金融机构应当对重要的外包服务提供商进行定期的风险评估，保持评估的独立性。至少在三年内覆盖

所有重要的服务提供商。评估内容包括：服务提供商合规情况、服务的执行效果等，评估结果应当作为服务提供商准入及退出的重要依据。

第二十四条 银行业金融机构内部审计部门应当定期开展信息科技外包风险管理审计工作，至少每三年对重要的外包服务活动进行一次全面审计。发生外包风险事件后应当及时开展专项审计。

第四章　信息科技外包管理

第一节　外包风险评估及准入

第二十五条 外包项目立项前，银行业金融机构应当审慎检查项目与信息科技外包战略的一致性，根据项目内容、范围、性质对其进行风险识别和评估，制定相应的风险处置措施，不因外包活动的引入而增加整体剩余风险。重大外包项目应向董事会、高管层报告。

第二十六条 银行业金融机构应当根据供应商关系管理策略，结合风险评估结果及服务提供商的准入标准，对备选服务提供商进行初步筛选，防范引入高机构集中度风险特点的服务提供商、或引入增加整体风险的服务提供商。

第二十七条 对于外包服务提供商为同业托管机构的情况，银行业金融机构可参照本节内容对其进行管理。

第二节　服务提供商尽职调查

第二十八条 对重要的服务提供商，银行业金融机构在与其签订合同前应当深入开展尽职调查，必要时可聘请第三方机构协助调查。

第二十九条 银行业金融机构在尽职调查时应当关注服务提供商的技术和行业经验，包括但不限于：服务能力和支持技术、服务经验、服务人员技能、市场评价、监管评价等。

第三十条 银行业金融机构在尽职调查时应当关注服务提供商的内部控制和管理能力，包括但不限于：内部控制机制和管理流程的完善程度、内部控制技术和工具等。

第三十一条 银行业金融机构在尽职调查时应当关注服务提供商的持续经营状况，包括但不限于：从业时间、市场地位及发展趋势、资金的安全性、近期盈利情况等。

第三十二条 对于关联外包，银行业金融机构不得因关联关系而降低对服务提供商的要求，应当在尽职调查阶段详细分析服务提供商技术、内控和管理水平，确认其有足够能力实施外包服务、处理突发事件等。

第三十三条 对于外包服务提供商为同业托管机构的情况，银行业金融机构可参照本节内容对其进行管理。

第三节　外包服务合同及要求

第三十四条 银行业金融机构在实施外包服务项目前，应当与服务提供商签订服务合同。合同应当根据外包服务需求、风险评估及尽职调查结果确定详细程度和重点。

第三十五条 银行业金融机构在合同或协议中应当明确以下内容，包括但不限于：

（一） 服务范围、服务内容、工作时限及安排、责任分配、交付物要求以及后续合作中的相关限定条件；

（二） 合规与内控要求，对法律法规及银行业金融机构内部管理制度的遵从要求、监管政策的通报贯彻机制、服务提供商的内控措施；

（三） 服务连续性要求，服务提供商的服务连续性管理目标应当满足银行业金融机构业务连续性目标要求；

（四） 银行业金融机构监控和检查的权利、频率，服务提供商配合其内、外部审计机构检查，及配合银行业监管机构检查的责任；

（五） 政策或环境变化因素等在内的合同变更或终止的触发条件，外包服务提供商在过渡期间应该履行的主要职责及合同变更或终止的过渡安排，包括信息、资料和设施的交接处置等过渡期间相关服务的安排；

（六） 外包服务过程中产生、加工、交互的信息和知识产权的归属权以及允许服务提供商使用的内容及范围，对服务提供商使用合法软、硬件产品的要求；

（七） 服务要求或服务水平条款，至少应当包括如下内容：外包服务的关键要素、服务时效和可用性、数据的机密性和完整

性要求、变更的控制、安全标准的遵守情况、技术支持水平等；

（八） 争端解决机制、违约及赔偿条款，至少包括如下内容：服务质量违约、安全违约、知识产权违约等，及在各种违约情况下的赔偿以及外包争端的解决机制；

（九） 报告条款，至少包括常规报告内容和报告频度、突发事件时的报告路线、报告方式及时限要求。

第三十六条 银行业金融机构应当在合同或协议中明确服务提供商在安全和保密方面的责任，以及针对安全及保密要求需采取的具体措施。包括但不限于：

（一） 禁止服务提供商在合同允许范围外使用或者披露银行业金融机构的信息，以防止信息被非授权使用；

（二） 在合同或协议中约定服务提供商对银行客户信息安全和银行客户权利的保护条款、事故处理方式及违约赔偿条款；

（三） 在合同或协议中约定服务提供商不得以所服务的银行业金融机构名义开展活动；

（四） 服务提供商接触银行业金融机构信息时，需满足安全和保密相关条款的要求；

（五） 在发生银监会规定的信息科技突发事件，或发生可能引发系统性、区域性银行业信息科技风险类突发事件时，服务提供商应及时向银行业金融机构报告，包括事件的影响以及处置和纠正措施。

第三十七条 银行业金融机构应当在合同或协议中明确要求服务提供商不得将外包服务转包和变相转包。在涉及外包服务分包时应当要求：

（一） 不得将外包服务的主要业务分包；

（二） 主服务提供商对服务水平负总责，确保分包服务提供商能够严格遵守外包合同或协议；

（三） 主服务提供商对分包商进行监控，并对分包商的变更履行通知或报告审批义务。

第四节 外包服务安全管理

第三十八条 银行业金融机构应当制定和落实信息安全管控措施，防范因外包活动引起的信息泄露、信息篡改、信息不可用、非法入侵、物理环境或设施遭受破坏等风险。具体措施包括：

（一） 对外包人员进行信息安全培训，提高风险管理意识，确保信息安全管控措施在外包服务过程中有效落实；

（二） 明确外包活动需要访问或使用的信息资产，包括场地、办公设施、计算机、服务器、软件、数据、信息、物理访问控制设备、账号、网络宽带、网络端口等，按“必需知道”和“最小授权”原则进行访问授权；

（三） 对重要或核心的信息系统开发交付物进行源代码检查和安全扫描；

（四） 定期对服务提供商进行安全检查，获取服务提供商自评估或第三方评估报告。

第三十九条 银行业金融机构对关联外包服务提供商定期进行的安全检查，不得以服务提供商的自评估替代，不得因关联关系而影响检查的独立性、客观性及公正性。

第四十条 银行业金融机构应当关注外包服务引入的新技术或新应用对现有治理模式及安全架构的冲击，及时完善信息安全管控体系，避免因新技术或应用的引入而增加额外的信息安全风险。

第五节 外包服务监控与评价

第四十一条 银行业金融机构应当对外包服务过程进行持续监控，要求服务提供商建立阶段性服务目标及任务，并跟踪任务的执行情况，及时发现和纠正服务过程中存在的各类异常情况。

第四十二条 银行业金融机构应当根据信息科技外包需求、合同、服务水平协议等建立明确的服务质量监控指标，并进行相应监控。常见指标包括：

（一） 信息系统和设备及基础设施的可用率、设备的开机率；

（二） 故障次数、故障解决率、故障的响应时间；

（三） 服务的次数、客户满意度；

（四） 各阶段业务需求的及时完成率、程序的缺陷数、需求变更率；

（五） 外包人员工作饱和率、外包人员的考核合格率。

第四十三条 银行业金融机构应当建立明确的服务目录、服务水平协议以及服务水平监控评价机制，并确保外包服务

监控基础数据和评价结果的真实性和完整性，且数据至少需保存到服务结束后一年。

第四十四条 银行业金融机构应当对服务提供商的财务、内控及安全管理进行持续监控，关注其因破产、兼并、关键人员流失、投入不足和管理不善等因素引发的财务状况恶化及内部管理混乱等情况，防范外包服务意外终止或服务质量的急剧下降。

第四十五条 银行业金融机构监控到异常情况时，应当及时督促服务提供商采取纠正措施，情节严重的或未及时纠正的，应当约谈服务提供商高管人员并限期整改。

第四十六条 外包服务结束时，银行业金融机构应当对服务提供商进行评价，评价结果应当作为服务提供商准入的重要参考依据。

第四十七条 对于关联外包，银行业金融机构董事会及高级管理层应当推动母公司或所属集团将外包服务质量纳入对服务提供商的业绩评价范围，建立外包服务重大事件问责机制。同时，应当要求服务提供商在其内部建立与外包服务水平相关的绩效考核机制。

第六节 外包服务中断与终止

第四十八条 银行业金融机构应当考虑信息科技外包的引入对业务连续性管理的影响，有针对性地完善业务连续性管

理计划，包括但不限于：

（一） 识别出重要业务所涉及的服务提供商和资源；

（二） 通过合同、协议等形式明确要求服务提供商提前准备并维护好相关资源；

（三） 对服务提供商业务连续性管理进行监控，并评价其管理水平；

（四） 在进行业务连续性计划演练时将相关的服务提供商纳入演练范围。

第四十九条 为降低外包突发事件的可能性及影响，银行业金融机构应当事先对业务连续性管理造成重大影响的外包服务建立风险控制、缓释或转移措施，包括但不限于以下内容：

（一） 在外包服务实施过程中持续收集服务提供商相关信息，尽早发现可能导致服务中断的情况；

（二） 与服务提供商事先约定在其服务质量不能满足合同要求的情况下获取其外包服务资源的优先权；

（三） 要求服务提供商制定服务中断相关的应急处理预案，如提供备份人员；

（四） 对于涉及重要业务的外包服务，银行业金融机构需考虑预先在其内部配置相应的人力资源，掌握必要的技能，以在外包服务中断期间自行维持最低限度的服务能力。

第五十条 银行业金融机构应当针对重要外包服务中断的场景，拟定相应的应急计划，并定期进行演练，考虑因素包括但不限于以下内容：

（一） 事件场景，如重要人员流失导致服务无法持续，服

务提供商主动退出，因资质变更、被收购、兼并或破产等原因导致的服务提供商被动退出等；

（二） 事件持续时间和恢复可能性；

（三） 事件影响范围和可能的应急措施；

（四） 服务提供商自行恢复服务的可能性和时间；

（五） 备选的服务提供商以及外包服务迁移方案；

（六） 外包服务过渡给银行业金融机构自行运作的可能性、时效及资源需求。

第五十一条 对于无法满足外包服务要求或发生重大事件的情况，银行业金融机构应当在充分评估其影响及制定退出计划的前提下，考虑主动要求服务提供商终止服务，情节特别严重的，可考虑取消准入资质，并报监管机构申请对其备案。对于关联外包，银行业金融机构不得因为关联关系而影响服务提供商退出机制的落实。

第五章 机构集中度风险管理

第五十二条 银行业金融机构应当依据服务提供商所承接外包服务的数量、金额在本行重要信息科技服务中的占比，服务提供商所承接外包服务在银行业服务市场占比情况，识别具有机构集中度特点的外包服务提供商。同时，还应识别服务提供商之间为集团子公司、关联公司或附属机构所产生的机构集中度风险。

第五十三条 银行业金融机构应当积极采用分散信息

科技外包活动、提高自主研发运行能力等形式，降低机构集中度，减少对外包服务提供商的依赖。

第五十四条 银行业金融机构应当要求具有机构集中度特点的外包服务提供商提供充分的证据，证明其内部控制和管理能力、持续运营能力等。

第五十五条 银行业金融机构应当要求具有机构集中度特点的外包服务提供商为银行业金融机构配备相对独立的资源，包括服务团队、场地、系统、设备等；并对资源进行定期检查，确保资源及时到位。

第五十六条 银行业金融机构应当要求具有机构集中度特点的外包服务提供商在外包服务中断应急预案中，明确外包服务的优先级，并进行服务中断应急演练，服务提供商应当至少参与服务交接、敏感信息处置等演练过程。

第五十七条 银行业金融机构应当特别加强对具有机构集中度特点的外包服务提供商的财务、内控、安全管理情况的持续监控，建立信息收集机制，及时掌握风险事件情况，防范外包服务意外终止或服务质量急剧下降对本机构产生大面积影响。

第五十八条 银行业金融机构应当对具有机构集中度特点的外包服务提供商增强监督频率与力度，必要时可指派专人进行现场监督。

第五十九条 对于具有机构集中度特点的外包服务提供商为同业托管机构的情况，银行业金融机构可参照本节内容对其进行外包管理。

第六章　跨境及非驻场外包管理

第一节　跨境外包风险管理

第六十条　跨境外包是指在境外其他国家或地区实施的信息科技外包服务活动。

第六十一条　跨境外包除具有本指引前述风险外，还包括由于某一国家或地区经济、政治、社会变化及事件而产生的国别风险，及由于外包实施场地远离银行业金融机构而产生的非驻场风险。

第六十二条　银行业金融机构应当充分了解并持续监控服务提供商所在国家或地区状况，通过建立业务连续性计划防范跨境外包所带来的国别风险。

第六十三条　银行业金融机构应当关注国外法律法规、监管要求对其获取服务提供商外包管理信息可能造成的影响。实施跨境外包应当以不妨碍银行业金融机构有效履行外包服务监控管理职能及监管机构延伸检查为前提。

第六十四条　银行业金融机构在选择跨境外包时，应当明确其所在国家或地区监管当局已与银监会签订谅解备忘录或双方认可的其他约定。

第六十五条　银行业金融机构在选择跨境外包时，还应当充分审查评估服务提供商保护客户信息的能力，并将其作为选

择服务提供商的重要指标。涉及客户信息的跨境外包，应当在符合监管法规政策并获得客户授权的前提下开展。

第六十六条 银行业金融机构在实施跨境外包时，其合同应当包括法律选择和司法管辖权的约定，明确争议解决时所适用的法律及司法管辖权，原则上应当要求服务提供商依照中国的法律解决纠纷。

第二节 非驻场外包风险管理

第六十七条 非驻场外包是指服务提供商不在银行业金融机构现场提供服务的外包形式。由于银行业金融机构不能对其内部控制及风险管理措施进行直接管控，应当在信息安全、知识产权保护、质量监控、法律合规等方面加强对服务提供商的风险管理。

第六十八条 银行业金融机构应当建立针对非驻场外包服务的内部控制及风险管理要求的最低标准，该标准应当作为选择服务提供商的最低要求。

第六十九条 银行业金融机构应当对重要的非驻场外包服务进行实地检查。实地检查原则上一年不少于一次，检查结果作为外包服务提供商项目考核及准入的重要指标。

第七十条 银行业金融机构应当加强对外包服务提供商非驻场外包服务内部控制、质量管理、信息安全的有效性评估，评估结果作为供应商准入的重要依据。对于高风险的服务提供商，

银行业金融机构应当责令其进行限期整改，对于逾期未改的服务提供商应当暂停或取消其服务资格。

第七十一条 对于非驻场外包服务提供商为同业托管机构的情况，银行业金融机构可以参照本节内容对其进行外包管理，但同业托管机构须将为其他同行业金融机构提供的信息科技外包服务视同自身信息科技服务的重要组成部分，不得区别对待，降低对自身提供外包服务的风险管控水平。

第七章 银行业重点外包服务机构风险管理要求

第七十二条 银行业重点外包服务机构是指集中为银行业金融机构提供外包服务，同时满足下述条件，如其外包服务失败可能导致银行业大面积数据损毁、丢失、泄露或信息系统服务中断，造成经济损失的机构，具体条件如下：

（一） 承担集中存贮客户数据的业务交易系统外包服务；或承担银行业金融机构客户资料、交易数据等敏感信息的批量分析或处理服务；或承担银行业金融机构数据中心、灾备中心机房及基础设施外包服务；且上述服务均为非驻场外包服务。

（二） 服务的法人银行业金融机构数量、服务合同金额占有本服务领域市场份额的三分之一以上；或服务的跨区域经营法人银行业金融机构数量达到 3 家或以上；或服务的其他类型法人银行业金融机构数量达到 10 家或以上。

第七十三条 银行业金融机构应当根据监管机构发布

的银行业重点外包服务机构风险提示，按照如下要求进行管理：

（一）银行业重点外包服务机构应当是中华人民共和国境内注册的独立法人实体，注册资本和实收资本不少于1000万，注册成立时间不少于3年。

（二）银行业重点外包服务机构应当拥有健全的组织架构，并针对所提供的外包服务建立有效的风险治理架构，至少应当建立由公司高级管理层直接领导、针对银行业金融机构外包服务的、专职信息科技风险管理团队，为持续的外包服务提供保证。

（三）银行业重点外包服务机构应当建立与所承担的服务范围和规模相适应的服务管理体系，建立完善的信息安全、服务质量、服务持续性等管理制度体系，拥有有效的检查、监控和考核机制，确保管理规范有效执行。

（四）银行业重点外包服务机构应当具有足够的技术能力、人力资源和设施、环境，满足外包服务的质量和安全管理要求。银行业重点外包服务机构承担的银行业金融机构外包服务场地应当设置在中国境内。

第七十四条 银行业金融机构应当要求银行业重点外包服务机构具有如下相关领域资质认证：

（一）具有完善的信息安全管理体系、业务连续性管理体系，并通过业界公认较为权威的信息安全管理和业务连续性管理资质认证。

（二）具有完善的质量管理体系，并通过业界公认较为权威的质量管理资质认证。

（三）承担银行业金融机构数据中心、灾备中心机房及基础

设施外包服务的银行业重点外包服务机构，其机房及基础设施应当达到国家电子计算机机房最高标准。

（四）承担集中存贮客户数据的业务交易系统外包服务，或承担银行业金融机构客户资料、交易数据等敏感信息的批量分析或处理服务的银行业重点外包服务机构，应当具有完善的运行服务管理体系，并通过业界公认较为权威的运行服务管理资质认证。

第七十五条 银行业金融机构应当在风险管理、审计方面对银行业重点外包服务机构提出如下要求：

（一）银行业重点外包服务机构应当具有信息科技风险的管理体系，有效识别、监测、评估和控制风险。银行业重点外包服务机构应当至少每季度向所服务的银行业金融机构报送外包风险监控报告，针对监控发现的潜在风险或风险事件，及时采取控制或缓释措施。

（二）银行业重点外包服务机构应当每年聘请独立的审计机构，对自身外包服务进行风险评估，年度风险评估报告需报送所服务的银行业金融机构，并抄送银监会或其派出机构。

（三）银行业重点外包服务机构应当对其外包服务团队成员进行背景调查，确保其过往无不良记录，且应当与项目成员签订保密协议，并保留至少 10 年的法律追诉期。

第八章 监督管理

第七十六条 银行业金融机构开展以下信息科技外包服务时，应当在外包合同签订前二十个工作日向银监会或其派出机构

报告，针对银行业金融机构信息科技外包风险，银监会及其派出机构可以采取风险提示、约见谈话、监管质询等措施。

（一）信息科技工作整体外包；

（二）数据中心或灾备中心整体外包；

（三）涉及将银行业金融机构客户资料、交易数据等敏感信息交由服务提供商进行分析或处理的信息科技外包；

（四）以非驻场形式实施的、集中存贮客户数据的业务交易系统外包；

（五）关联外包；

（六）涉及跨境的信息科技外包；

（七）其他银监会认为重要的信息科技外包。

第七十七条 银行业金融机构信息科技外包活动中发生如下重大事件时，应当在两个工作日内向银监会或其派出机构报告。

（一）银行业金融机构客户信息等敏感数据泄露；

（二）数据损毁或者重要业务运营中断；

（三）由于不可抗力或服务提供商重大经营、财务问题，导致或可能导致多家银行业金融机构外包服务中断；

（四）其他重大的服务提供商违法违规事件；

（五）银监会规定需要报告的其他重大事件。

第七十八条 银行业金融机构在开展年度外包风险管理评估工作后，应当将年度风险评估报告报送银监会或其派出机构。

第七十九条 银监会及其派出机构对银行业金融机构信息科技外包工作进行监督和检查，监督检查结果纳入对银行业金融机构的监管评级。

第八十条 对于风险较高的信息科技外包服务，银监会或其派出机构可以要求银行业金融机构暂缓、中止该类外包服务，直至银行业金融机构、外包服务提供商有效改正。

第八十一条 银行业金融机构违反本指引规定的，银监会或其派出机构可要求其纠正或采取替代方案，并视情况予以问责。因管理过失导致外包活动严重危及银行业金融机构稳健运行、损害存款人和其他客户合法权益的，依法追究银行业金融机构管理责任。

第八十二条 银监会实行银行业信息科技外包服务活动风险监测机制，定期对银行业金融机构发布银行业重点外包服务机构名单和风险提示，防范因高机构集中度外包服务导致的系统性、区域性信息科技风险。

第八十三条 银监会应当对具有机构集中度特点的银行业金融机构信息科技外包服务进行重点风险监测、评估，根据需要，可以要求银行业金融机构与重点外包服务机构会谈，就其外包服务活动和风险的重大事项作出说明。

第八十四条 银监会应当组织银行业金融机构实地核查银行业重点外包服务机构承担的银行业金融机构信息科技服务活动，原则上每两年进行一次，也可以委托其他第三方机构审计的形式实施。

第八十五条 银监会可以根据银行业金融机构信息科技服务活动风险评估和实地核查结果，对银行业金融机构发出监管提示，要求其督促银行业重点外包服务机构对风险问题实施整改。

第八十六条 银行业重点外包服务机构应当配合银行业金融机构及银监会的风险监测和实地核查。

第八十七条 银监会组织相关银行业金融机构对银行业信息科技外包服务提供商建立服务管理记录，并对其进行风险评估和评级。

第八十八条 服务提供商在外包服务中存在以下情形的，银监会定期向银行业发布服务提供商风险预警，公布机构名单、服务信息等，要求银行业金融机构禁止相关服务提供商承担银行业信息科技外包服务，禁止期至少为两年。外包服务提供商两年内仍未整改的，延长其禁止期。

（一）违反国家法律、法规和监管政策，情节严重的；

（二）窃取、泄露银行业金融机构敏感信息，情节严重的；

（三）因管理过失，多次发生重要信息系统服务中断或数据损毁、丢失、泄露事件的；

（四）服务质量低下并给多家银行业金融机构造成损失，多次提示仍未整改的；

（五）对风险监测和实地检查发现的问题，逾期仍未整改的；

（六）存在其他违法违规行为，或发生其他重大信息科技风险事件的。

第八十九条 银监会负责监督银行业金融机构对信息科技外包服务提供商实施准入管理。对于存在重大风险的外包活动，银行业金融机构应当立即评估外包的适当性，对信息科技外包服务提供商进行风险预警提示，要求其进行整改并设定期限；逾期未整改的，禁止其承担信息科技外包服务。

第九章 附则

第九十条 本指引由银监会负责解释、修订。

第九十一条 本指引自公布之日起施行。