银行保险机构信息科技外包风险监管办法

第一章　总则

第一条 为规范银行保险机构的信息科技外包活动，加强信息科技外包风险管控，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》《中华人民共和国保险法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规，制定本办法。

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，保险集团（控股）公司、保险公司、保险资产管理公司、金融资产管理公司适用本办法。银保监会及其派出机构监管的其他金融机构参照本办法执行。

第三条 本办法所适用的信息科技外包，是指银行保险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。

银行保险机构与其他第三方合作当中涉及银行保险机构重要数据和客户个人信息处理的信息科技活动，按照本办法相关要求进行管理，法律法规另有要求的除外。

第四条 银行保险机构应当建立与本机构信息科技战略目标相适应的信息科技外包管理体系，将信息科技外包风险纳入全面风险管理体系，有效控制由于外包而引发的风险。

第五条 银行保险机构在实施信息科技外包时应当坚持以下原则：

（一）不得将信息科技管理责任、网络安全主体责任外包；

（二）以不妨碍核心能力建设、积极掌握关键技术为导向；

（三）保持外包风险、成本和效益的平衡；

（四）保障网络和信息安全，加强重要数据和个人信息保护；

（五）强调事前控制和事中监督；

（六）持续改进外包策略和风险管理措施。

第二章　信息科技外包治理

第六条 银行保险机构应建立覆盖董（理）事会、高管层、信息科技外包风险主管部门、信息科技外包执行团队的信息科技外包及风险管理组织架构，明确相应层级的职责，确保信息科技外包治理架构权责清晰、运转高效、制衡充分。

第七条 银行保险机构董（理）事会或其授权设立的专业委员会应负责推动建立信息科技外包及其风险管理体系、审批信息科技外包战略、审议重大外包决策，高级管理层应负责制定信息科技外包战略，明确信息科技外包风险主管部门和信息科技外包执行团队，明确信息科技外包及其风险管理职责，审议信息科技外包管理流程及制度，监控信息科技外包及其风险管理成效。

第八条 银行保险机构应指定信息科技外包风险主管部门，该部门主要职责包括：

（一）根据机构总体风险政策和外包战略，制定信息科技外包风险管理策略、制度和流程；

（二）统筹信息科技外包风险的识别、评估、监测、预警、报告及处置工作；

（三）制定保障外包服务持续性的应急管理方案，并定期组织实施演练；

（四）监督、评价外包执行团队的管理工作，并督促外包风险管理的持续改善；

（五）向董（理）事会（或其专门委员会）或高级管理层汇报信息科技外包相关风险及管理情况。

第九条 银行保险机构应在信息科技管理部门或信息科技外包活动执行部门内部建立信息科技外包执行团队，并配备足够的具有相应能力和经验的人员履行以下职责：

（一）落实信息科技外包战略；

（二）执行信息科技外包管理制度与流程；

（三）执行服务提供商准入、尽职调查、服务评价和退出管理工作，建立并维护服务提供商关系管理策略；

（四）持续监测外包服务的水平和质量，及时处理服务提供商出现的相关违规和用户投诉；

（五）对外包过程中的关键管理活动进行监控及分析，定期与信息科技外包风险主管部门沟通外包活动及有关风险情况。

第十条 银行保险机构应当基于机构的业务战略、信息科技战略、总体外包战略、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，包括但不限于：外包原则和策略、不能外包的职能、资源能力建设方案等。

第十一条 银行保险机构应当明确不能外包的信息科技职能。涉及信息科技战略管理、信息科技风险管理、信息科技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。

第十二条 银行保险机构应当建立信息科技外包活动分类管理机制，针对不同类型的外包活动建立相应的管理和风控策略。信息科技外包原则上划分为咨询规划类、开发测试类、运行维护类、安全服务类、业务支持类等类别。

第十三条 银行保险机构应对信息科技外包活动及相关服务提供商进行分级管理，对重要外包和一般外包采取差异化管控措施。下列信息科技外包活动原则上属于重要外包：

（一）信息科技工作整体外包，仅保留必要的管理团队和核心职能；

（二）数据中心（机房）整体外包；

（三）涉及基础设施和信息系统整体架构发生重大变化的信息科技外包；

（四）核心业务系统开发测试和运行维护的整体外包；

（五）信息科技战略规划（含中长期规划）咨询外包；

（六）安全运营的整体外包；

（七）涉及集中存储或处理银行保险机构重要数据和客户个人敏感信息的外包；

（八）直接影响实时服务、影响账务准确性的重要信息系统外包；

（九）其它对机构业务运营具有重要影响的外包。

第十四条 银行保险机构应考虑重要外包终止的可能性，并制定退出策略。退出策略应至少明确：

（一）可能造成外包终止的情形；

（二）外包终止的业务影响分析；

（三）终止交接安排。

第三章　信息科技外包准入

第十五条 银行保险机构应当充分评估拟开展的信息科技外包活动与信息科技外包战略的一致性，充分评估拟开展的信息科技外包活动相关风险，就是否实施外包作出审慎决策。重要外包应至少向高管层报告并经过审批。

第十六条 银行保险机构应根据信息科技外包战略，结合风险评估情况，明确服务提供商的准入标准，对备选服务提供商进行筛选，审慎引入集中度风险较高或增加机构整体风险的服务提供商。

第十七条 银行保险机构应在签订合同前，对重要外包的备选服务提供商深入开展尽职调查，必要时可聘请第三方机构协助调查。在服务提供商经营状况未发生重大变化的前提下，尽职调查结果原则上一年内有效。尽职调查应包括但不限于：

（一）服务提供商的技术和行业经验，人员及能力；

（二）服务提供商的内部控制和管理能力；

（三）服务提供商的网络和信息安全保障能力；

（四）服务提供商的持续经营状况；

（五）服务提供商及其母公司或实际控制人遵守国家和银保监会相关法律法规要求的情况；

（六）服务提供商过往配合银行保险机构审计、评估、检查及监管机构监督检查情况；

（七）服务提供商与银行保险机构的关联性。

第十八条 对于符合重要外包条件的非驻场外包，应当进一步重点调查如下内容：

（一）服务提供商对银行保险机构与其他机构的设施、系统和数据是否有明确、清晰的边界；

（二）服务提供商是否有管理制度和技术措施保障银行保险机构数据的完整性和保密性；

（三）服务提供商对涉及银行保险机构的服务器、存储、网络设备、操作系统、数据库、中间件等软硬件基础设施是否具有最高访问权限；

（四）服务提供商是否拥有或可能拥有业务系统的最高管理权限或访问权限，是否能够浏览、获取重要数据或客户个人敏感信息；

（五）服务提供商是否有完善的灾难恢复设施和应急管理体系，是否有业务连续性安排；

（六）服务提供商是否存在不正当竞争或规避监管的情形。

第十九条 银行保险机构在选择跨境外包时，应当充分评估服务提供商所在国家或地区的政治、经济、社会、法律、文化等经营环境。涉及信息跨境存储、处理和分析的，应遵守我国有关法律法规的规定。

第二十条 对于关联外包和同业外包，银行保险机构不得降低对服务提供商的要求，严格防范利益冲突和利益输送。

第二十一条 银行保险机构在信息科技外包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、服务要求、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，服务质量考核评价约定。

（二）合规、内控及风险管理要求，对法律法规及银行保险机构内部管理制度的遵守要求，监管政策的通报贯彻机制。

（三）服务持续性要求，服务提供商的服务持续性管理目标应当满足银行保险机构业务连续性目标要求。

（四）银行保险机构对服务提供商进行风险评估、监测、检查和审计的权利，及服务提供商承诺接受银保监会对其所承担的银行保险机构外包服务的监督检查。

（五）合同变更或终止的触发条件，合同变更或终止的过渡安排。

（六）外包活动中相关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）资源保障条款。

（八）安全保密和消费者权益保护约定，包括但不限于：禁止服务提供商在合同允许范围外使用或者披露银行保险机构的信息，服务提供商不得将银行保险机构数据以任何形式转移、挪用或谋取外包合同约定以外的利益。

（九）争端解决机制、违约及赔偿条款，跨境外包应明确争议解决时所适用的法律及司法管辖权，原则上应当选择中国仲裁机构、中国法院管辖，适用中国法律解决纠纷。

（十）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。

第二十二条 银行保险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或变相转包。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服务提供商进行监控，并对分包服务提供商的变更履行通知或报告审批义务。

第四章　信息科技外包监控评价

第二十三条 银行保险机构应当对外包服务过程进行持续监控，及时发现和纠正服务过程中存在的各类异常情况。

第二十四条 银行保险机构应当建立明确的信息科技外包服务目录、服务水平协议以及服务水平监控评价机制，确保相关监控信息和评价结果的真实性和完整性，且数据至少保存到服务结束后三年。

第二十五条 银行保险机构应当对信息科技外包服务建立服务效能和质量监控指标，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；

（二）故障次数、故障解决率、故障的响应时间、故障的解决时间；

（三）服务的次数、客户满意度；

（四）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；

（六）网络和信息安全指标、业务连续性指标。

第二十六条 银行保险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。

第二十七条 银行保险机构监控到信息科技外包服务出现异常情况时，应当及时督促服务提供商采取纠正措施；情节严重或未及时纠正的，应当及时约谈服

务提供商高管人员并限期整改。对于逾期未整改的服务提供商，应当暂停或取消其服务资格，并向银保监会或其派出机构报告。

第二十八条 对于关联外包，银行保险机构董（理）事会和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。

第二十九条 银行保险机构应在信息科技外包服务到期前，就是否继续外包进行评估决策。外包服务结束时，银行保险机构应对服务提供商进行评价，评价结果作为服务提供商后续准入的重要参考依据。对具有持续性特点的外包服务，银行保险机构终止外包或更换服务提供商前，应制定周密的退出和交接计划。

第五章　信息科技外包风险管理

第三十条 银行保险机构应建立并持续完善风险管理制度和流程，充分识别并评估信息科技外包可能产生的风险，包括但不限于：

（一）科技能力丧失。过度依赖外包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）数据泄露、丢失和篡改。因服务提供商的不当行为或其服务的信息系统遭受网络攻击，导致银行保险机构重要数据或客户个人信息泄露、丢失和篡改。

（四）资金损失。因服务提供商的不当行为或其服务的信息系统遭受网络攻击，导致银行保险机构客户资金被盗取。

（五）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，使得信息科技服务水平下降。

（六）可能导致的战略、声誉、合规等其他风险。

第三十一条 针对可能给业务连续性管理造成重大影响的重要外包服务，银行保险机构应当事先建立风险控制、缓释或转移措施，包括但不限于：

（一）事先制定退出策略和供应链安全保障方案，并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或服务质量下降的情况；

（二）明确措施和方法，在服务提供商服务质量不能满足合同要求的情况下，保障获取其外包服务资源的优先权；

（三）要求服务提供商提供必要的应急和灾备资源保障，制定应急处理预案并在预案中明确为银行保险机构提供应急响应和恢复的优先级，原则上应为最高级；

（四）组织服务提供商参与应急计划编制和应急演练，至少每年在综合性演练或专项演练中纳入一个或多个服务提供商开展一次相关演练；

（五）考虑预先在银行保险机构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。

第三十二条 银行保险机构应当制定和落实网络和信息安全管理措施，包括但不限于：

（一）对服务提供商和外包人员进行网络和信息安全教育或培训，增强网络和信息安全意识，服务提供商应与银行保险机构签订安全保密协议，外包人员应签署安全保密承诺书；

（二）明确外包活动需要访问或使用的信息资产，按“必需知道”和“最小授权”原则进行访问授权，严格管控远程维护行为；

（三）对信息系统开发交付物（含拥有知识产权的源代码）进行安全扫描和检查；

（四）对客户信息、源代码和文档等敏感信息采取严格管控措施，对敏感信息泄露风险进行持续监测；

（五）对服务提供商所提供的模型、算法及相关信息系统加强管理，确保模型和算法遵循可解释、可验证、透明、公平的原则；

（六）定期对外包活动进行网络和信息安全评估。

第三十三条 银行保险机构应识别对本机构具有集中度风险的外包服务及其提供商，积极采用分散外包活动、注重外包项目知识产权保护、提高自身研发运维能力、储备潜在替代服务提供商等手段，减少对个别外包服务提供商的依赖，降低集中度风险。

第三十四条 银行保险机构应当对符合重要外包标准的非驻场外包服务进行实地检查，原则上每三年覆盖所有重要的非驻场外包服务。对具有行业集中度性质的服务提供商，银行保险机构可采取联合检查、委托检查等形式，减少重复性工作，减轻服务提供商的检查负担。

第三十五条 银行保险机构每年应当至少开展一次全面的信息科技外包风险管理评估，并向董（理）事会或高级管理层提交评估报告。

第三十六条 银行保险机构应当开展信息科技外包及其风险管理的审计工作，定期对信息科技外包活动进行审计，至少每三年覆盖所有重要外包。发生重大外包风险事件后应当及时开展专项审计。银行保险机构应承担内部审计职能和责任，内部审计项目可委托母公司或同一集团下属子公司实施，或聘请独立第三方实施。

第六章　监督管理

第三十七条 银行保险机构开展以下信息科技外包活动时，应当在外包合同签订前二十个工作日向银保监会或其派出机构的信息科技监管部门报告（目录见附件）：

（一）信息科技工作整体外包；

（二）数据中心（机房）整体外包；

（三）涉及基础设施和信息系统整体架构发生重大变化的外包；

（四）信息科技战略规划（含中长期规划）咨询外包；

（五）符合重要外包条件的非驻场外包、关联外包和跨境外包；

（六）其他银保监会认为重要的信息科技外包。

第三十八条 银行保险机构信息科技外包活动中发生以下重大风险事件时，应当按照相关突发事件监管报告要求，向银保监会或其派出机构报告：

（一）银行保险机构重要数据或客户个人信息泄露；

（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保险机构外包服务中断；

（四）重要外包服务非正常中断、终止或其服务提供商非正常退出；

（五）因服务提供商不当行为或其服务的信息系统遭受网络攻击或其他原因，造成银行保险机构客户重大资金损失；

（六）发现重大的服务提供商违法违规事件；

（七）银保监会规定需要报告的其他重大事件。

相关突发事件报告要求中没有规定的，在 24 小时内向银保监会或其派出机构报告。

第三十九条 银保监会及其派出机构对银行保险机构信息科技外包风险进行独立评估，对银行保险机构信息科技外包工作进行监督和检查，并纳入监管综合评价体系。对于检查发现涉嫌违法事项的有关单位和个人，依照相关法律规定实施延伸检查。

第四十条 银保监会及其派出机构持续监测银行业保险业信息科技外包风险状况，建立行业和区域集中度风险监测与核查机制，对重大或共性风险及时向行业发布风险提示，积极防范因信息科技外包可能引发的区域性、系统性风险。根据风险状况，银保监会及其派出机构可以要求银行保险机构与服务提供商会谈，就其外包服务和风险相关的重大事项作出说明。

第四十一条 银保监会及其派出机构可组织或责令银行保险机构对承担银行保险机构信息科技外包服务的服务提供商进行现场核查，也可由银行保险机构委

托其他第三方机构以审计的形式实施。银保监会建立信息共享机制，及时向行业通报现场核查情况。

第四十二条 对于经监管评估、监督检查或现场核查风险较高的信息科技外包服务，银保监会及其派出机构可以对银行保险机构采取风险提示、约见谈话、监管质询、要求暂缓和停止相关外包活动等措施。对具有重大违法违规情形的服务提供商，银保监会可通报行业，必要时将有关情况移交司法机关。

第四十三条 银行保险机构违反本办法要求的，银保监会及其派出机构依法予以纠正，并视情况予以问责或处罚。

第七章　附则

第四十四条 本办法所称关联外包，是指银行保险机构的母公司或其所属集团子公司、关联公司或附属机构作为服务提供商，为其提供信息科技外包服务的行为。

同业外包，是指依法设立的由银保监会监管的银行保险机构为其他同行业金融机构提供外包服务的行为。

跨境外包，是指服务提供商在境外其他国家或地区实施信息科技外包服务的行为。

非驻场外包，是指服务提供商不在银行保险机构场所提供服务的外包形式。

重要数据，包括但不限于客户资料、交易数据、商业秘密等，参见国家法律法规和国家标准对重要数据的相关定义。

客户个人信息和敏感信息，参见国家法律法规和国家标准对个人信息的相关定义。

第四十五条 本办法由银保监会负责解释和修订。

第四十六条 本办法自公布之日起施行。《银行业金融机构信息科技外包风险监管指引》（银监发〔2013〕5号）、《中国银监会办公厅关于加强银行业金融机构信息科技非驻场集中式外包风险管理的通知》（银监办发〔2014〕187号）、

《中国银监会办公厅关于开展银行业金融机构信息科技非驻场集中式外包监管评估工作的通知》（银监办发〔2014〕272号）同时废止。

附件：1.银行保险机构信息科技外包监管报告材料目录

2.信息科技外包服务类型参考

附件1

银行保险机构信息科技外包监管报告

材料目录

一、外包服务基本情况，包括：

1. 外包服务名称；

2. 外包服务类型：咨询规划类、开发测试类、运行维护类、安全服务类、业务支持类等；

3. 外包服务的主要内容；

4. 实施方式：驻场外包、非驻场外包；

5. 影响的业务类型：渠道管理类、客户管理类、产品管理类、财务管理类、决策支持类、共享支持类等；

6. 外包服务起止时间。

二、服务提供商基本情况，包括：

1. 服务提供商全称、国别；

2. 尽职调查报告；

3. 法人代表；

4. 注册资本；

5. 上级机构/母机构；

6. 成立时间；

7. 企业性质；

8. 统一社会信用代码。

三、外包风险评估报告。

银保监会规定的其他材料。

附件 2

信息科技外包服务类型参考

咨询规划类。包括但不限于：信息科技战略规划（含中长期规划）咨询，数据中心（机房）整体建设咨询和规划，信息科技治理（含数据治理）、信息科技风险管理体系、信息安全管理体系、业务连续性管理体系等管理类咨询和规划，重要信息系统架构和建设相关的咨询和规划，新兴技术应用咨询和规划。

开发测试类。包括但不限于：软硬件开发和测试外包（含人力外包），软件即服务形式的外包。

运行维护类。包括但不限于：数据中心（机房）物理环境的托管或运行维护，软硬件基础设施托管或运行维护，应用系统运行维护，电子机具运行维护，终端等办公设备的运行维护，以及涉及以上运行维护的人力外包。

安全服务类。包括但不限于：安全运营服务，安全加固服务，安全设备运行维护，安全日志处理与分析，安全测试服务，密钥管理及运行维护，数据安全服务，以及涉及以上服务的人力外包。

业务支持类。包括但不限于：市场拓展、业务运营（集中作业、呼叫中心等）、企业管理、资产处置、数据处理、数据利用等业务外包或第三方合作当中涉及银行保险机构的重要数据或客户个人信息处理的信息科技活动，法律法规另有要求的除外。