pwc 普华永道

把控风险变局，筑底开放生态

—《银行保险机构信息科技外包风险监管办法》研读

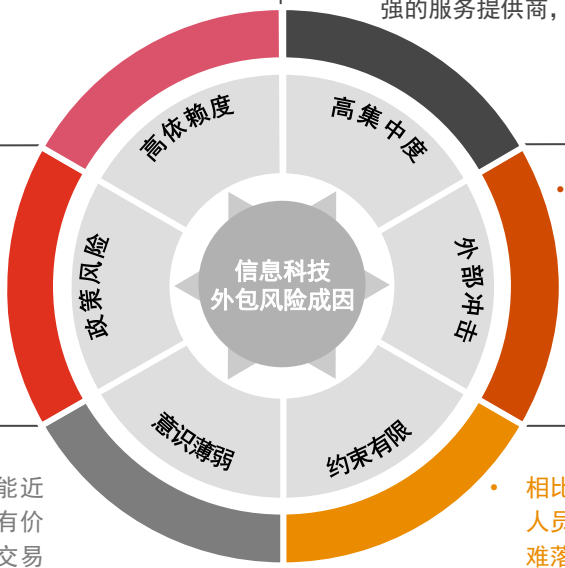
为进一步加强银行保险机构信息科技外包风险监管，促进银行保险机构提升信息科技外包风险管控能力，银保监会于2021年12月30日发布了《银行保险机构信息科技外包风险监管办法》（“银保监办发[2021]141号”，以下简称“141号文”）。141号文共7章46条，将作为当前金融机构信息科技外包风险管理的指挥棒，对银行保险机构、其他金融机构和服务提供商等均具有重要意义。141号文已自公布之日起正式施行，这对全面风险管理体系和日常工作提出了更高要求。普华永道初步分析了银行保险机构在响应141号文落地时可能面临的难点及应对建议，以供参考。

一、背景与概述

受到行业特性和宏观经济环境的影响，金融机构信息科技外包风险的表现兼具外包常见的人员风险、操作风险，也具备行业独特的集中度风险、监管风险等。

- 金融机构业务和产品种类繁多，信息科技与系统管理任务重，对信息科技外包依赖程度较高。
- 金融机构由于自身运营和管理需要，以及成本压力，使用外包服务较为普遍。

- 随着行业高度竞争和洗牌，重点服务提供商的规模不断扩张，单个服务提供商可能承接较多金融机构的服务需求。
- 金融机构出于服务质量、风险管理压力、节省管理资源的考虑，倾向选择业内排名靠前、实力较强的服务提供商，集中度进一步提高。



- 金融机构信息科技外包监管持续趋严。
- 金融科技新业态不断涌现，各类服务和合作类型具有较大概率被纳入信息科技外包范畴，增加了潜在的政策风险。

- 近年来疫情爆发和国际摩擦加剧、“黑天鹅”事件时有发生，服务提供商面临较大的生存压力，经营情况和服务水平都会受到影响。

- 外包人员在提供服务中，能近距离接触金融机构的大量有价值的敏感信息，如客户和交易信息，极易造成信息泄露。
- 服务提供商自身的内控体系成熟度、风险管理能力和风险意识水平往往低于金融机构，难以有效识别外包人员主动或被动的不当行为。

- 相比较自身员工，金融机构对外包人员的管理难度更高，管理要求更难落实到位。外包人员的归属感、责任感较弱，或只注重短期目标。
- 外包人员流动性较大，不利于岗位知识技能传递，难以保证长期持续高效和高质量的服务水平。

金融科技创新浪潮为金融机构与服务提供商之间带来多种新的合作形式，也使外包的定义和边界范围变得模糊。自2014年以来，监管再未直接发布信息科技外包风险专项监管指引，但监管动向并未放松，而是呈现更为细化和定向的趋势；加之行业内外部环境持续快速变化，为金融机构全面风险管理的有效性带来诸多变数与冲击：

1

外包服务的类型逐渐从传统的人力外包、项目外包转变为技术输出、技术合作，尤其是在金融机构数字化转型、构建开放生态的过程中，这一趋势更为明显。

2

在同期其他主题下的一系列监管指引中，外包或对外合作仍是热点，反映持续的监管导向，例如对外合作中不允许管理职责外包，并在数据安全和个人信息保护中重点关注数据的“委托处理”等。

3

金融机构对外包风险事件往往防不胜防。例如针对外包违规催收、数据公司侵权或不当获取、使用个人隐私数据的曝光和处罚，造成金融机构声誉风险事件频发。新冠疫情则在业务连续性管理、服务提供商持续经营、远程办公和服务相关网络安全等方面带来新的风险。

二、《银行保险机构信息科技外包风险监管办法》关注点

相较于2013年发布的《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，以下简称“5号文”），以及2014年针对非驻场外包发布的《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，以下简称“187号文”），近期的141号文充分反映了8年来金融行业、科技和监管导向变化的时代背景，其内容主要变化总结如下：

1

把控趋势和明确导向

- 结合监管热点，补充重要数据和个人信息保护、网络安全、消费者权益保护、信息跨境、模型算法管理等内容，与其他法律法规联动；
- 细化和拓展了信息科技外包服务类型，扩大定义范围。

2

完善治理和管理职责

- 细化董事会、高管层、外包风险主管部门和外包执行团队职责；
- 信息科技外包风险主管部门负责外包风险管理策略和统筹管理，补充风险监测、预警、报告和处置职能及外包相关服务持续性管理要求。

3

落实风控与管理闭环

- 重申信息科技外包风险纳入全风管理，完善重要外包定义和过程管控；
- 做好外包事中监督、持续监测服务水平和质量，终止、退出和交接、到期评估，以及优化协议、尽调、集中度风险和业务连续性管理要求。

1. 以信息科技外包过程中的网络安全、数据安全和个人信息保护作为核心导向

141号文第一条将2017年生效的《网络安全法》、以及2021年生效的《数据安全法》和《个人信息保护法》纳入依据，与《银行业监督管理法》、《商业银行法》和《保险法》置于同等重要的位置，可预见网络安全、数据安全和个人信息保护在未来一个较长时期内，仍将是金融业信息科技风险管理的核心主题。

第三条对信息科技外包进行定义时，除沿用5号文中的传统定义外，补充了“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”，使得银行保险机构以往多项与外部机构的合作，或服务采购，可能被纳入到信息科技外包活动范畴中，大大拓展了管理外延。

第五条中对银行保险机构信息科技外包原则的阐述中，将网络安全主体责任作为和信息科技管理责任并列的对象，明令不得外包，以及将“保障网络和信息安全，加强重要数据和个人信息保护”作为重要原则之一。

第十九条要求跨境外包活动中，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。预计此条未来将与国家网信办、工信部所发布的个人信息与数据出境安全、网络安全和数据安全审查相关法规等形成关联。

第二十一条要求信息科技外包合同或协议应当明确内容中，较5号文明确新增资源保障条款、安全保密和消保约定、跨境外包争议解决机制等内容。

信息科技外包合同或协议内容要求

1. 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。
2. 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。
3. 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。
4. 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。
5. 合同变更或终止的触发条件，合同变更或终止的过渡安排。
6. 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。
7. **资源保障条款**。
8. **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。
9. 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。
10. 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。

第三十条对潜在信息科技外包风险识别和评估中，补充了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，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，以及客户资金被盗取的风险。

第三十二条列示了银行保险机构应当指定和落实网络和信息安全管理措施，较5号文相比，在与服务提供商和外包人员签订安保协议或承诺书、严格管控远程维护、敏感信息泄露风险防控、服务提供商的模型、算法和相关信息系统管理等方面，新增或明确了相关内容。

网络和信息安全管理措施

1. 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；**
2. 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；
3. 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；
4. 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；
5. 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；**
6. 定期对外包活动进行**网络和信息安全评估。**

此外，141号文附则中对重要数据、客户个人信息和敏感信息注明参考国家法律法规和国家标准相关定义。此前多项法律法规、监管指引、国家标准和金融行业标准中已对个人信息或金融数据委托给外部机构处理的行为，做出明确规范要求，141号文与之有效联动。

文件类型	文件名称	参考条文内容
法律法规	**《个人信息保护法》**	第二十一条 个人信息处理者委托处理个人信息的，应当**与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。**受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。未经个人信息处理者同意，受托人不得转委托他人处理个人信息。
国家标准	**GB/T 35273-2020 信息安全技术 个人信息安全规范**	9.1 委托处理 个人信息控制者委托第三方处理个人信息时，应符合以下要求： a. 个人信息控制者作出委托行为，**不应超出已征得个人信息主体授权同意的范围**或应遵守5.6所列情形； b. 个人信息控制者应对委托行为进行**个人信息安全影响评估**，确保受委托者达到11.5的**数据安全能力要求；** c. 受委托者应： 1. 严格按照个人信息控制者的要求处理个人信息。受委托者因特殊原因未按照个人信息控制者的要求处理个人信息的，应及时向个人信息控制者反馈； 2. 受委托者确需再次委托时，应事先征得个人信息控制者的授权； 3. 协助个人信息控制者响应个人信息主体基于8.1~8.6提出的请求； 4. 受委托者在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件的，应及时向个人信息控制者反馈； 5. 在委托关系解除时不再存储相关个人信息。 **d. 个人信息控制者应对受委托者进行监督，方式包括但不限于：** **1. 通过合同等方式规定受委托者的责任和义务；** **2. 对受委托者进行审计。** e. 个人信息控制者应准确记录和存储委托处理个人信息的情况； f. 个人信息控制者得知或者发现受委托者未按照委托要求处理个人信息，或未能有效履行个人信息安全保护责任的，应立即要求受托者停止相关行为，且采取或要求受委托者采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险。必要时个人信息控制者应终止与受委托者的业务关系，并要求受委托者及时删除从个人信息控制者获得的个人信息。
行业标准	**JR/T 0171-2020 个人金融信息保护技术规范**	6.1.4.4 委托处理 金融业机构因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（包含外包服务机构与外部合作机构）处理时，具体技术要求如下： a. 委托行为**不应超出已征得个人金融信息主体授权同意的范围**或遵循 7.1 中对于征得授权同意的例外所规定的情形，并准确记录和保存委托处理个人金融信息的情况。 **b. C3 以及 C2 类别信息中的用户鉴别辅助信息，不应委托给第三方机构进行处理。**转接清算、登记结算等情况，应依据国家有关法律法规及行业主管部门有关规定与技术标准执行。 c. 对委托处理的信息应采用**去标识化**（不应仅使用加密技术）**等方式进行脱敏处理**，降低个人金融信息被泄露、误用、滥用的风险。 d. 应对委托行为进行**个人金融信息安全影响评估**，并确保受委托者具备足够的数据安全能力，且提供了足够的安全保护措施。 e. 应对第三方机构等受委托者进行监督，方式包括但不限于： • 依据 7.2.1 的要求，通过合同等方式规定受委托者的责任和义务； • 依据 7.4.2 的要求，对受委托者进行安全检查和评估。 f. 应对外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）开展技术检测，确保其个人金融信息收集、使用行为符合约定要求；并对其收集个人金融信息的行为进行审计，发现超出约定行为及时切断接入。

2. 完善外包治理和风险管理相关方的职责

141号文第六条要求建立包括四方（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，并在第七至第九条进行了列举；尤其是在信息科技外包风险主管部门的职责中，提出加强统筹管理、应急管理相关职能，进一步将信息科技外包风险管理责任和目标落地。

董（理）事会或其授权设立的专业委员会

- 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；
- 对于关联外包，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。

高级管理层

- **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；
- 对于关联外包，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。

信息科技外包风险主管部门

- **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**；
- **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；
- **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；**
- 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；
- 开展全面的信息科技外包风险管理评估，向董（理）事会或高级管理层汇报信息科技外包相关风险及管理情况、提交评估报告。

信息科技外包执行团队

- 落实信息科技外包战略；
- 执行信息科技外包管理制度与流程；
- 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；
- **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；**
- 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。

3. 细化和拓展信息科技外包活动分类，分级管理给出重要外包判断原则和管理要求

141号文第十二条要求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。相较5号文中将信息科技外包分类为研发咨询、系统运行维护和业务外包中的信息科技活动三类，141号文的划分较为全面地囊括了业内现有各类信息科技服务活动形式，并以“涉及银行保险机构的重要数据或客户个人信息处理”作为兜底原则。

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

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。

上述各类信息科技外包活动中，银行保险机构应关注战略规划等管理类咨询和规划服务、以及数字化转型过程中可能出现的新兴技术应用咨询规划。开发测试类中，软件即服务（即“SaaS”）形式以往可能会因为系统不在银行保险机构内部落地而未被纳入外包。安全服务类作为新增类型，需注意安全运营的整体外包属于重要外包范畴。业务支持类中，数据利用服务可能会导致部分从外部机构向银行保险机构侧提供数据输入的服务，被纳入外包管理范畴。

141号文第十三条要求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。重要外包判断原则如下：

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

数据中心（机房）整体外包

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

核心业务系统开发测试和运行维护的整体外包

信息科技战略规划（含中长期规划）咨询外包

安全运营的整体外包

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

直接影响实时服务、影响账务准确性的重要信息系统外包

其它对机构业务运营具有重要影响的外包

141号文其他条文以重要外包的完整生命周期为主线，串联起各主要环节和场景的管理要求，线索清晰：

要点	条文内容	分析解读
退出策略	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： 1. 可能造成外包终止的情形； 2. 外包终止的**业务影响分析**； **3. 终止交接安排。**	银行保险机构以往较重视事前尽调与事中风险评估等工作，但对外包活动中断、中止或交接环节的规范要求重视可能不够，主要关注服务交付和结项。本条结合第二十九条对外包终止的要求，共同形成外包周期的完整闭环后端管理要求。
外包决策	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。**	5号文中仅要求“重大外包项目应向董事会、高管层报告。”141号文中明确要求至少应经高管层审批。
尽职调查	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： 1. 服务提供商的技术和行业经验，**人员及能力**； 2. 服务提供商的内部控制和管理能力； **3. 服务提供商的网络和信息安全保障能力；** 4. 服务提供商的持续经营状况； **5. 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；** **6. 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；** **7. 服务提供商与银行保险机构的关联性。**	5号文中未对尽调结果有效期做出要求。141号文落地后，针对提供持续数年的重要服务提供商或将要求每年开展尽职调查。141号文中强调尽职调查范围需包括服务提供商的网络和信息安全保障能力，以及过往国家和监管法律法规要求的合规遵从情况等，对服务提供商提出了更高要求。

要点	条文内容	分析解读
非驻场外包附加要求	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： 1. 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； 2. 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； 3. 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； 4. 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；** 5. 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； 6. 服务提供商是否存在不正当竞争或规避监管的情形。	本条承继了187号文中对非驻场集中式外包服务商要求；但141号文中仅定义非驻场外包，去掉了“非驻场集中式外包”概念，统一以重要外包条件作为标准。明确敏感信息范围包括重要数据或客户个人敏感信息（187号文中为“客户敏感信息”）。
业务连续性管理	**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： 1. **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； 2. 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； 3. 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；** 4. **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；** 5. 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。	本条要求针对重要外包需事先制定退出策略并持续监控，同时将目前逐渐成为热点的供应链安全纳入管控。较5号文内容，本条细化了服务提供商需承担的应急响应和保障职责；同时明确要求银行保险机构将重要外包服务提供商纳入到应急计划编制和演练等环节。信息科技外包风险主管部门（常为业务连续性管理主管部门）需对此予以关注。此外第三十三条要求银行保险机构通过知识产权保护、储备潜在替代服务提供商等手段减少对个别服务提供商的依赖和降低集中度风险，应一并考虑。

要点	条文内容	分析解读
实地检查	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。	本条融合了5号文中对重要外包服务提供商定期风险评估（三年全覆盖）和重要非驻场外包服务实地检查要求（每年），可操作性更强。
外包风险审计	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。**	本条将5号文中“至少每三年对重要的外包服务活动进行一次全面审计”调整为“至少每三年覆盖所有重要外包”，增加了灵活性；并将风险事件专项审计触发标准调整为“重大外包风险事件”。银行保险机构内审部门需关注监管对内审职能独立承担的重申，以及可委托关联方实施审计，而聘请第三方机构则应关注独立性要求。
事前报告	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）： 1. 信息科技工作整体外包； 2. 数据中心（机房）整体外包； 3. **涉及基础设施和信息系统整体架构发生重大变化的外包；** 4. **信息科技战略规划（含中长期规划）咨询外包**； 5. **符合重要外包条件**的非驻场外包、关联外包和跨境外包； 6. 其他银保监会认为重要的信息科技外包。	本条将事前报告要求聚焦于重要外包（5号文中要求涉及“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”、“关联外包”以及“涉及跨境的信息科技外包”应进行事前报告）。同时对比第十三条中重要外包判断标准，可了解对各类重要外包的侧重点。

要点	条文内容	分析解读
重大风险事件报告	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： 1. 银行保险机构**重要数据或客户个人信息泄露；** 2. 数据损毁或者重要业务运营中断； 3. 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; **4. 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**； **5. 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**； 6. 发现重大的服务提供商违法违规事件； 7. 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。	本条补充了需及时向监管机构进行报告的事项范围，例如将5号文中作为被泄露对象“客户信息等敏感数据”拓展为“重要数据或客户个人信息”，并增加对重要外包服务和服务提供商的中断、终止和非正常退出场景，以及服务提供商侧出现的系统遭受网络攻击造成重大资金损失等高风险场景。此外银行保险机构需关注报告时限较5号文要求的两个工作日内显著缩短，需做好应对。

三、银行保险机构在141号文落地所面临挑战与应对建议

除部分标准在未来落地过程中还需结合业内管理实践，进行参考和厘清外，141号文整体要求较为清晰明确，与其他法律法规联动紧密。诸多变化使得银行保险机构信息科技外包风险管理面临巨大挑战，合规压力显著提升。普华永道初步分析了银行保险机构在响应141号文落地时可能面临的难点，并提出应对建议。

难点1：
可能将银行保险机构原先对外合作中涉及重要数据和个人信息处理的科技活动，以及原来属于合作性质的机构纳入外包管理体系，涉及合作模式的转换，对机构和服务提供商均属新课题。

外包管理外延扩大

1

应对建议1：
建议银行保险机构评估目前可能会被新纳入外包管理的服务与合作机构，与监管要求进行对标，识别管理差距并开展内部沟通。优先梳理分析涉及内外敏感信息交互的管理情况，充分利用现有管理抓手，尽快启动必要改进或风险缓释机制。

难点2：
外包风险主管部门需与外包执行团队紧密协同，加强事中监控与预警、退出/终止、完善业务连续性与应急处置、报告等环节，并推动管理和治理层明确和落实相应责任。

管理体系完善，闭环与协同

2

应对建议2：
建议银行保险机构尽快开展对标和排查，加快机制优化和落地，充分利用现有信息科技风险管理体系，完善各道防线分工与协同，并取得高层支持，统一内部各方认识，尽快形成行动计划。

难点3：
因外包外延扩大被新纳入管理的合作方必须接受银行保险机构外包风险管理监督。原有服务提供商也需在个保、网安、消保等领域面对更高标准。银行保险机构对服务提供商侧不具有决策权却承担合作风险。

推动服务提供商侧改进

3

应对建议3：
建议外包风险主管部门，牵头合规等部门梳理现有外包合作协议中相关内容，与外包执行团队做好分工和调度，提前与服务提供商进行沟通，各方就合规提升目标和步骤尽快达成共识。

难点4：
保险机构、保险资产管理公司、金融资产管理公司等需遵守141号文的机构，此前在信息科技外包风险管理组织及职责、管理策略、分类管理、制度流程、日常运营等方面较银行业机构可能存在一定差异。

保险和其他金融机构体系建设

4

应对建议4：
对新纳入本办法监管范围的金融机构，建议尽快着手对自身信息科技外包活动和外包风险管理体系全面盘点，以识别和排查不足之处，落地合规体系建设完善工作。

普华永道可以协助的领域

141号文已自公布之日起正式施行，这对全面风险管理体系和日常工作提出了更高要求。普华永道在包括信息科技外包风险管理在内的金融行业信息科技风险管理和全面风险管理领域具备成熟的方法论、完善的工具和经验丰富的团队。我们可在包括不仅限于如下方面为贵机构提供协助：

- 信息科技外包风险管理合规全面梳理诊断
- 信息科技外包治理、运行机制及风险管理机制建设咨询
- 信息科技外包供应商准入及定期考核评估咨询
- 信息科技外包风险评估
- 信息科技外包定期管理评价或审计
- 重大外包风险事件专项审计
- 科技外包服务的服务提供商风险监测、现场核查

如果您的客户在以上领域面临新规落地的压力和挑战，或需要我们的服务，欢迎与我们联系：

联系我们：

张立钧
普华永道中国金融业主管合伙人
电话：+86 (755) 8261 8882
邮箱：james.chang@cn.pwc.com

杨丰禹
普华永道中国金融行业风险与控制服务主管合伙人
电话：+86 (755) 8261 8186
邮箱：philip.yang@cn.pwc.com

北区

梁震
普华永道中国金融行业风险与控制服务合伙人
电话：+86 (10) 6533 5979
邮箱：zhen.liang@cn.pwc.com

李文蔚
普华永道中国金融科技服务高级经理
电话：+86 (10) 6533 7283
邮箱：will.ww.li@cn.pwc.com

刘翰林
普华永道中国金融行业风险与控制服务合伙人
电话：+86 (10) 6533 5206
邮箱：harrison.liu@cn.pwc.com

曹一伸
普华永道中国金融科技服务经理
电话：+86 (10) 8553 1053
邮箱：chelsea.y.cao@cn.pwc.com

南区

丘振球
普华永道中国金融行业风险与控制服务合伙人
电话：+86 (20) 3819 2325
邮箱：micheal.qiu@cn.pwc.com

刘晓莉
普华永道中国金融行业风险与控制服务副总监
电话：+86 (755) 8261 8441
邮箱：ashley.liu@cn.pwc.com

中区

陈彦
普华永道金融行业中国风险与控制服务合伙人
电话：+86 (21) 2323 2307
邮箱：eric.y.chen@cn.pwc.com

王润
普华永道金融行业中国风险与控制服务合伙人
电话：+86 (21) 2323 3550
邮箱：speed.wang@cn.pwc.com

www.pwccn.com