

# 汉坤法律评述

2026 年 9 月 4 日

北京 | 上海 | 深圳 | 杭州 | 武汉 | 海口 | 香港 | 新加坡 | 纽约 | 硅谷 | 伦敦

## 云上方圆（五）：金融机构上云的治理框架与要求

作者：权威 | 朱俊 | 李珣 | 夏迎雨 | 郑博 | 洪松

随着金融机构数字化转型持续推进，云计算的应用范围已经由办公、人力等内部支持场景，逐步扩展至客户渠道、风险管理、数据分析、业务运营及人工智能应用。

对于金融机构而言，一项上云项目可能同时涉及信息科技外包、数据委托处理、重要信息系统投产及变更、网络产品和服务采购以及业务连续性管理。此外，近期中国人民银行、国家金融监督管理总局、中国证监会和国家外汇管理局联合发布《金融业网络安全管理办法（征求意见稿）》，其中亦将云计算服务采购情况纳入供应链安全管理的范畴。

云服务有助于提升资源配置效率和系统弹性，同时也可能使金融机构的基础设施、运行平台、系统运维和数据处理在不同程度上依赖外部服务商。由此，云平台故障、配置变更、供应链异常及服务商经营风险，均可能向金融机构的业务运行传导，进而影响金融业务连续性和客户权益保障。

在此背景下，金融机构上云的监管重点正在由单一系统安全向覆盖采购、迁移、运行和退出的全生命周期治理延伸。本文拟从金融云的监管定位出发，对金融机构上云中的实务与合规关注要点进行梳理。

### 一、金融机构上云的主要形态

#### （一）金融云的内涵与外延

“金融云”是对金融领域云计算应用的概括性称谓，其在金融行业标准和市场实践中的含义并不完全一致。《云计算技术金融应用规范技术架构》（JR/T0166—2020）将“金融云”作为“金融团体云”的同义词，主要指仅供金融机构共享使用并承载金融业务系统的团体云。市场实践中的“金融云”则通常具有更广泛的含义，金融机构建设或者使用的私有云、金融团体云、混合云以及相关云服务，均可能被统称为“金融云”。本文为便于讨论，采用后一种广义用法。

市场上还存在“金融行业云”“金融专属云”“金融专区”“托管云”等产品名称。这些名称主要用于描述产品定位或者合作方案，未必与标准中的部署模式一一对应。识别一项上云项目的具体形态，通常需要分别考察云资源的部署模式、服务商交付的服务类别以及云平台的建设和运营方式。

#### （二）金融机构常见的云部署模式

部署模式主要反映云资源由哪些使用者使用和共享，以及相关资源由谁控制。目前市场中常见的部署模式包括以下几类：

| 部署模式  | 基本概念                                                           | 常见市场操作形式                                                                 |
|-------|----------------------------------------------------------------|--------------------------------------------------------------------------|
| 私有云   | 仅供一家金融机构使用，云资源由该机构控制。“私有”主要体现为资源专用和机构控制，并不以云平台是否部署在机构自有机房为唯一标准 | 金融机构采购服务器、存储、网络和云平台软件，由服务商完成建设、集成和交付；平台可由金融机构自行运维，也可另行采购升级、维保或者托管运维服务    |
| 金融团体云 | 由特定金融机构共同使用和共享，承载金融业务系统，底层资源可以由云服务商或者使用者控制                     | 云服务商、金融机构建设统一资源池，并据此形成公共基础设施、公共接口、公共应用等公共服务，金融机构以租户身份通过专线、控制台或者接口接入并使用资源 |
| 混合云   | 由两种以上部署模式组成，各云环境保持相对独立，同时通过网络和管理机制实现连接                         | 将私有云与金融团体云等环境通过专线、接口、统一身份认证或者云管理平台连接，并根据业务和技术需求配置不同系统、数据及计算任务            |
| 公有云   | 可以向任意云服务使用者提供服务，共享资源池通常由云服务商控制，不同租户之间采取逻辑隔离                    | 云服务商通过标准产品目录、在线控制台或者 API 提供云主机、存储、数据库、内容分发和人工智能等服务，通常采用订阅或者按量计费方式        |

表 1 金融机构常见的云部署模式

“专属云”或者“金融专区”既可能对应由单一金融机构控制的私有云，也可能只是金融团体云或公有云中的专属资源区或者逻辑隔离租户，仍需根据资源是否共享以及实际控制关系进行识别。“多云”则主要描述金融机构同时采购多个云服务商的产品，属于技术和采购策略，也不构成一种独立的部署模式。

市场实例也反映了部署模式与项目名称之间的差异。例如，某银行公开介绍的全栈分布式金融云平台由两朵私有云构成，并在同一平台上提供 IaaS、PaaS 和 SaaS 能力；某金融基础设施机构对其产品的公开介绍则同时涵盖行业云、私有云和混合云等多种场景。因此，仅凭“金融云”这一项目名称或者产品品牌，通常无法确定其实际部署模式。

### （三）云服务类别和新型服务形态

服务类别主要反映服务商向金融机构交付的具体技术层级。同一种部署模式可以同时提供多个级别的服务。例如，私有云既可以只提供计算、存储和网络资源，也可以在基础设施之上继续建设数据库、容器平台和业务应用。

| 服务类别或形态 | 主要交付内容               | 常见市场操作形式                                                         |
|---------|----------------------|------------------------------------------------------------------|
| IaaS    | 计算、存储、网络和虚拟化等基础设施能力  | 金融机构采购云主机、物理机、块存储、对象存储、虚拟网络、负载均衡和 GPU 算力等产品，通常按照实例、容量、流量或者使用时长计费 |
| PaaS    | 应用开发、测试、部署和运行所需的平台能力 | 金融机构采购数据库、中间件、容器、分布式数据处理、大数据和人工智能开发平台，通常按照节点、实例、资源规模或者服务期限计费     |

| 服务类别或形态 | 主要交付内容                    | 常见市场操作形式                                                                       |
|---------|---------------------------|--------------------------------------------------------------------------------|
| SaaS    | 可以直接使用的完整应用软件             | 金融机构通过租户账户使用办公、人力资源、客户服务、业务管理等应用，并完成必要的参数配置、数据导入和系统对接，通常按照账户、模块、期限或者业务量订阅      |
| MaaS    | 模型训练、精调、推理、评测或者智能体开发等模型能力 | 金融机构通过 API 调用共享模型，采购专属模型实例或者模型开发平台，也可以取得模型及运行环境进行本地部署，通常按照调用量、Token、算力或者服务期限计费 |

表 2 金融机构上云的服务形态、交付内容及操作形式

《云计算技术金融应用规范技术架构》（JR/T0166—2020）将 IaaS、PaaS 和 SaaS 作为三类主要云服务，同时还列举了网络即服务（NaaS）和数据存储即服务（DSaaS）等具体类别；MaaS 则是随着大模型应用发展形成的市场服务形态。

服务类别与交付方式同样需要分别识别。举例而言，某银行业数据分类分级大模型同时提供本地部署和在线 MaaS 服务，其中，MaaS 描述的是机构取得何种模型能力，本地部署或者在线调用则描述该能力如何交付；对于作为用户的金融机构而言，该产品既可以连同运行环境在机构内部部署，也可以进行在线调用。

## 二、金融机构上云前的项目准备：明确建设运营方式与基础项目事实

### （一）建设运营方式：直接影响合规要求适用范围

建设和运营方式主要解决金融机构上云项目中底层资源投入、平台建设和日常运营的问题。

目前，市场上常见的安排包括：

- **自建自营。**金融机构自行采购软硬件、建设云平台并负责日常运营；
- **服务商建设、金融机构运营。**服务商完成私有云建设和系统集成，验收后由金融机构接管；
- **服务商建设并托管运维。**服务商除建设平台外，还持续承担监控、升级、故障处理和技术支持；
- **在线订阅。**金融机构通过租户、账户或者 API 使用服务商提供的 IaaS、PaaS、SaaS 或者 MaaS；
- **混合云或者多云管理。**金融机构分别采购不同云环境或者不同服务商的能力，并通过专线、接口或者统一管理平台连接。

上述方式可以组合使用。例如，金融机构可以采购由服务商建设的私有云，再将部分运维工作委托给第三方；也可以在私有云之外接入数据库、灾备或者模型服务。因此，同样被称为“私有云”或者“金融专区”的项目，所涉及的采购、集成、运维和数据处理安排可能并不相同。

上述建设和运营方式的不同，会使上云项目在资源控制、技术交付、数据处理和交易结构等方面呈现不同特征，并可能对应不同的信息科技外包、数据安全和供应链管理要求。因此，在讨论具体合规要求之前，需要先回答四个基础问题：

“谁在上云”、“哪些系统上云”、“哪些数据进入云环境”以及“相关服务实际由哪些主体提

供”。

## （二）“四张清单”：梳理业务方案并形成基础事实判断

建设和运营方式明确后，结合具体项目情况，金融机构可以分别形成主体、系统、数据和供应链四张清单，分别回答以下问题：

- **主体清单**。参与上云的主体范围，以及哪些主体对采购、系统、数据和安全负责；
- **系统清单**。准备上云的系统范围，以及哪些系统或者模块暂不迁移；
- **数据清单**。拟进入云环境的数据范围，以及可以访问或者处理前述数据的主体范围；
- **供应链清单**。实际提供云服务的主体范围，并进一步明确完整的履约链条。

| 清单类型 | 应当记录的关键事实                                                                                                                                                                                                                                                      | 重点判断问题                                                                                                                                                                               |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 主体清单 | <ul style="list-style-type: none"> <li>(1) 主体牌照类型及业务范围、所在地；</li> <li>(2) 集团既有关联交易安排，例如内部服务；</li> <li>(3) 主体职责，例如采购/签约/运营/数据处理/运维/安全管理等；</li> <li>(4) 是否已被认定为关键信息基础设施运营者及相关系统范围；</li> <li>(5) 是否涉及境外机构或者境外技术支持</li> </ul>                                       | <ul style="list-style-type: none"> <li>(1) 适用的分业及属地监管规则</li> <li>(2) 金融机构内部的责任主体及责任边界</li> <li>(3) 集团内服务、关联方服务及信息科技外包的定性</li> <li>(4) 内部审议及监管报告、备案或者审查要求</li> </ul>                  |
| 系统清单 | <ul style="list-style-type: none"> <li>(1) 系统业务功能，例如客户服务、资金、账务、交易、风险管理；</li> <li>(2) 系统服务对象，例如 toB/toC/内部使用；</li> <li>(3) 现有及目标技术服务架构、部署位置和控制权限；</li> <li>(4) 上下游系统及外部服务依赖情况；</li> <li>(5) 技术要求，例如峰值容量、实时性、最大可容忍中断时间；</li> <li>(6) 迁移、切换、回退及旧系统停用安排</li> </ul> | <ul style="list-style-type: none"> <li>(1) 系统重要性及监管分级</li> <li>(2) 上云范围及云上云下管理边界</li> <li>(3) 部署模式、服务类别与系统要求的适配</li> <li>(4) 系统迁移、投产、变更及退出管理</li> <li>(5) 信息科技外包的定性及重要性分级</li> </ul> |

| 清单类型  | 应当记录的关键事实                                                                                                                                                               | 重点判断问题                                                                                                            |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| 数据清单  | (1) 数据来源、处理目的及业务用途；<br>(2) 现有分类分级及个人信息属性；<br>(3) 数据量级和保存期限；<br>(4) 存储、备份、灾备及流转地点；<br>(5) 金融机构、云服务商、分包商和技术支持人员的访问权限；<br>(6) 是否存在远程运维、境外访问或者数据出境；<br>(7) 数据返还、迁移和删除方式     | (1) 数据分类分级及敏感程度<br>(2) 云服务项下的数据处理关系<br>(3) 数据访问、存储、传输及权限控制<br>(4) 重要数据、个人信息及敏感个人信息保护要求<br>(5) 风险评估、监管报告、备案及数据出境程序 |
| 供应链清单 | (1) 各主体实际提供的服务、合同关系和交付地域；<br>(2) 控制的基础设施、平台、账号、密钥、日志及数据权限；<br>(3) 资质许可、安全能力、行业经验、财务状况和持续经营能力；<br>(4) 分包及转委托层级；<br>(5) 供应商、技术栈和部署区域的集中程度；<br>(6) 替代服务商、数据及配置导出、迁移协助和退出条件 | (1) 服务商准入、资质及安全能力<br>(2) 外包分级、分包及转委托管理<br>(3) 网络安全审查及供应链安全要求<br>(4) 供应商集中度及技术锁定风险<br>(5) 业务连续性、服务替代及退出能力          |

表 3 金融机构上云前进行基础事实判断的“四张清单”

完成上述盘点后，金融机构应当对于以下关键问题具备初步结论：

- 项目上云的系统/模块范围；
- 采购、签约和投产前应当履行的内部审议、监管报告/备案/核查程序；
- 服务商需要满足的准入、合同、技术、持续运营和退出要求。

在上述事实确认后，金融机构可以进一步判断具体项目适用的分业监管、信息科技外包、系统管理、数据安全和供应链管理要求，明确合规上云路径。

### 三、金融机构上云的主要合规要求

一项上云项目可能同时涉及多类监管要求，例如同时构成信息科技外包、数据委托处理、重要信息系统建设或变更以及第三方产品和服务采购；此外，金融机构还应关注其所持有牌照对应的特定行业监管要求。

### （一）常见类型金融机构可能涉及的特定行业监管规则

不同金融监管条线对系统独立、外包范围、数据处理和服务商管理的关注重点有所不同。同一云服务方案用于不同金融机构时，可能形成不同的准入条件、报告程序和合同要求。

| 适用主体或者业务领域    | 主要监管要求                                                                                                                                                                     | 对上云方案的主要影响                                             |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| 银行保险机构        | <ul style="list-style-type: none"> <li>■ 信息科技管理责任、网络安全主体责任和数据安全主体责任不得外包；</li> <li>■ 分别识别重要外包、特定外包事前报告、敏感级及以上数据安全评估以及批量敏感级及以上数据委托处理事前报告等要求</li> </ul>                       | 同步完成外包定性及分级、数据分类分级和报告判断，并保留系统控制、监督审计和替代退出能力            |
| 证券期货核心机构和经营机构 | <ul style="list-style-type: none"> <li>■ 重要信息系统上线、变更和下线应当履行风险评估、测试和回退程序；</li> <li>■ 证券公司和公募基金管理公司还应确保重要信息系统始终处于自身控制范围；</li> <li>■ 提供特定重要信息系统服务的机构依法备案</li> </ul>           | 机构需掌握重要系统架构、业务逻辑和操作流程，并对服务商参与运维、安全管理及系统变更设置控制措施        |
| 非银行支付机构       | <ul style="list-style-type: none"> <li>■ 具备必要且独立的业务系统、设施和技术；</li> <li>■ 业务系统及备份存放境内；</li> <li>■ 境内交易处理、资金结算和数据存储在境内；</li> <li>■ 涉及资金安全、信息安全等的核心业务和技术服务不得委托第三方处理</li> </ul> | 重点识别云平台是否承载支付核心业务、关键技术服务和相关数据，并核实境内部署及机构实际控制能力         |
| 人民银行业务领域数据处理者 | <ul style="list-style-type: none"> <li>■ 适用范围按照人民银行承担监管职责的业务领域及相关数据确定；</li> <li>■ 向其他数据处理者提供、委托处理或者共同处理重要数据前应当开展风险评估，委托处理还需落实合同、监督、外包管理及处理完成后的数据转移和删除要求</li> </ul>         | 支付清算、征信、反洗钱、银行间市场和跨境人民币等业务数据，可能与机构适用的其他分业规则叠加适用，需要逐一排查 |
| 其他持牌主体        | <ul style="list-style-type: none"> <li>■ 按照相应牌照规则核对系统独立、核心职能、数据保存、外包管理和属地监管要求</li> </ul>                                                                                   | 结合信托、财务公司、金融租赁、保险中介、基金销售和地方金融组织等具体规则逐项确定               |

表 4 主要金融机构上云监管关注事项

相较而言，银行保险机构的主要抓手是重要外包和数据安全管理；证券基金机构更强调重要信息系统持续处于自身控制以及信息技术系统服务机构管理；支付机构则存在较为明确的核心业务和技术服务禁止委托边界。

同一机构也可能同时适用多组规则。例如，商业银行处理支付清算业务数据时，需要同时核对银行保险监管规则和人民银行业务领域数据规则；金融机构被认定为关键信息基础设施运营者的，还应叠加关键信息基础设施安全保护和网络安全审查要求。

## （二）服务商参与可能构成信息科技外包

服务商是否承接了原由金融机构负责的信息科技活动，是外包定性的核心。具体可以依次判断：

- **外包定性：**服务商是否承担系统开发测试、平台运维、安全运营、数据备份或者其他持续性信息科技活动；
- **重要性分级：**所涉系统和数据是否重要，服务中断是否会影响核心业务、账务准确性、客户服务或者数据安全；
- **监管程序：**是否需要履行内部审批、事前报告或者其他监管程序；
- **责任保留：**金融机构是否保留信息科技管理、网络安全、数据安全和内部审计等不得转移的责任及职能。

以银行保险机构为例，《银行保险机构信息科技外包风险监管办法》第 13 条列举了数据中心整体外包、导致基础设施和信息系统整体架构发生重大变化的外包、核心业务系统整体开发测试和运行维护等重要外包情形。该办法第 37 条另行规定了合同签订前二十个工作日需要报告的外包事项。两条规定的适用范围并不完全相同，重要外包仍需逐项核对是否触发事前报告。

此外，软硬件或者标准化产品采购本身不一定会构成外包；如采购同时包含持续运维、安全管理或者数据处理服务，应当对相关服务部分单独判断。

## （三）重要系统迁移需要履行投产变更程序

系统上云可能同时涉及运行环境、部署地点、技术架构、外部依赖和运维方式的变化。因此，金融机构在确定迁移方案时，不能仅将其作为一般的数据搬迁或者设备替换，而应结合适用的系统管理规则依次判断：

- **系统属性：**拟上云系统是否属于核心系统、重要信息系统或者其他需要重点管理的系统；
- **变更性质：**相关安排属于系统新建上线、重大改造、运行变更、机房或者部署地点调整，还是旧系统下线；
- **投产准备：**上线或者切换前是否需要完成风险评估、测试、数据核验、备份、应急处置及回退验证；
- **程序要求：**是否需要履行内部审议、投产审批、监管报告或者其他前置程序。

如果上云迁移构成重要信息系统新建上线、重大改造或者运行变更，金融机构需要在采购、服务商准入和外包管理程序之外，同步完成相应的系统投产变更程序。测试和风险评估的范围应结合实际情况框定；涉及旧系统停用的，还应一并明确数据迁移、历史数据保存、资源释放和回退安排。

以证券期货行业为例,《证券期货业网络和信息安全管理办法》要求核心机构和经营机构在重要信息系统新建上线、运行变更或者下线移除前评估技术和业务风险,并制定风险防控、应急处置和回退方案,复核验证相关结果;上线或者变更前还应制定并执行全面测试方案。可能对证券期货市场安全平稳运行产生较大影响的,还应按照该办法履行相应的报告程序。

#### (四) 数据上云需要判断数据类型和处理关系

数据上云的对象不限于生产数据库,还可能包括日志、备份、快照、缓存、开发测试数据以及故障排查过程中形成的临时副本。对于 MaaS 等模型服务,还可能包括提示词、训练或者精调数据、模型输入输出和运行日志。金融机构需要结合系统架构和实际数据流转过程,依次判断以下事项:

- **数据范围和存在形态:** 明确哪些数据将在云环境中上传、存储、备份、传输或者生成,并将日志、快照、缓存、测试数据和临时副本一并纳入判断;对于经过脱敏、汇总或者加工的数据,还需核实其能否关联至原始数据或者特定主体;
- **行业数据分类分级:** 按照适用的金融行业规则和机构内部数据目录,识别相关数据的业务类别和安全级别,并判断其中是否包含核心数据、重要数据或者敏感级及以上数据;
- **个人信息属性:** 另行判断相关数据是否构成个人信息或者敏感个人信息。金融行业的数据分类分级与《个人信息保护法》下的个人信息分类属于不同判断体系,不能相互替代;
- **服务商的实际访问权限:** 核实主服务商、底层云厂商、分包商及技术支持人员能否通过控制台、特权账号、密钥管理、日志服务、远程运维或者故障排查接触数据明文。由金融机构持有密钥且服务商仅保存密文,与服务商可以解密、调用或者导出数据,对处理关系和风险判断可能产生不同影响;
- **各参与方的数据处理关系:** 根据各方实际决定和实施数据处理的方式,区分委托处理、共同处理、向其他数据处理者对外提供等情形;如果服务商超出金融机构指示留存或者再利用相关数据的,可能影响原有处理关系的判断,金融机构需要据此重新核对处理依据、数据范围以及相应的合同和评估要求;有分包商或者关联方参与履约的,还需继续判断是否发生转委托或者新的对外提供;
- **存储地域和跨境链路:** 核实数据、备份和日志的实际存储地点,以及是否存在境外技术支持人员远程访问、境外控制台调用、跨境日志分析或者境外灾备。存在相关安排的,应进一步判断是否构成向境外提供数据,并核对相应的数据出境和行业监管要求。

上述判断会直接影响金融机构需要采取的管理措施。涉及个人信息委托处理的,应当按照《个人信息保护法》约定处理目的、期限、方式、个人信息种类、保护措施和双方权利义务,对受托人的处理活动进行监督,并对转委托作出控制;构成共同处理或者向其他个人信息处理者提供的,则需分别核对相应的责任约定、告知、同意及其他处理要求。

对于银行保险机构,处理敏感级及以上数据,或者开展对数据主体有较大影响的委托处理、共同处理、转移、公开、共享等活动,应当按照《银行保险机构数据安全管理办法》事先开展数据安全评估;涉及批量敏感级及以上数据委托处理的,还需核对在数据处理或者合同签署前至少二十个工作日履行报告的要求。委托处理数据时,应明确数据范围、处理条件、返还或者删除方式,并限制受托方未经同意转委托、对外共享或者将数据用于合同约定之外的加工和训练。

涉及中国人民银行业务领域重要数据的,向其他数据处理者提供、委托处理或者共同处理前,还应

当按照《中国人民银行业务领域数据安全管理办法》开展风险评估，并落实合同约定、受托方监督以及处理完成后的数据转移和删除要求。

完成上述判断后，金融机构可以确定允许进入云环境的数据范围、服务商及分包商的访问边界，以及需要履行的评估、报告、合同控制和跨境程序，并据此开展后续的服务商准入审查。

## （五）服务商准入需要覆盖完整服务链条

### 1. 服务商准入主体管理

金融机构对云服务商开展准入管理时，审查对象除了直接签订合同的主体之外，还应视项目需求，进一步识别实际参与服务交付的底层云厂商、IDC 或者网络服务商、平台及软件提供商、托管运维商、分包商、关联方和境内外技术支持团队，并明确各主体实际提供的服务、掌握的系统权限以及可能接触的数据范围。

### 2. 服务商审查内容管理

金融机构对服务商审查的具体内容也需要根据金融机构类型、服务内容和项目重要程度确定。

#### （1）服务商尽调基础要求

金融机构应根据其适用的特定监管规则，判断对服务商尽调时所需关注的具体事项。例如：

- 就银行保险机构的重要信息科技外包而言，《银行保险机构信息科技外包风险监管办法》要求机构在合同签订前对备选服务商开展尽职调查，重点考察其技术和行业经验、内部控制、网络和信息安全保障能力、持续经营状况、合规情况，以及配合审计、评估和监管检查的情况。
- 证券基金经营机构委托信息技术服务机构提供服务前，也需按规定对服务机构及相关信息系统开展内部审查，并预先制定更换服务提供方的流程及预案。

#### （2）分包/转委托要求

项目涉及分包或者转委托的，还需进一步核实分包范围、分包层级和变更机制。例如：

- 银行保险机构的信息科技外包合同应当禁止转包或者变相转包；涉及分包的，不得将外包服务的主要业务分包，主服务商应当对服务水平负总责，并对分包商进行监控，履行相应的变更通知或者报告审批义务。
- 证券基金信息技术服务机构亦不得在服务对象不知情的情况下转委托第三方提供服务。金融机构需要通过尽调材料和合同安排掌握实际服务链条，并将适用的安全、数据、事件报告和检查配合要求落实至相关参与方。

#### （3）关注服务商集中度/替代能力

金融机构在服务商准入过程中还应关注集中度和替代能力，包括同一服务商是否承载多个重要系统，底层资源是否集中于同一云平台或者同一区域，以及在服务中断或者服务商经营状况发生变化时是否存在可行的替代方案。

银行保险机构还应按照信息科技外包监管要求识别外包集中度风险，并结合项目情况采取分散外包、提高自身研发运维能力或者储备替代服务商等风险控制措施。

此外，金融机构被认定为关键信息基础设施运营者的，还需根据具体采购项目预判采购云计算服务是否影响或者可能影响国家安全；符合《网络安全审查办法》规定情形的，应当申报网络安全审查。

完成上述审查后，金融机构可以形成服务商（含分包商）清单及对应关键事项审查结果，并据此确定服务商准入条件、合同控制措施和退出预案。

## 四、金融云合同与全生命周期管理

金融机构上云过程中涉及的监管要求最终需要落实到云服务合同以及迁移、运行和退出等具体环节，故应当结合上云系统、数据范围、服务模式和供应链结构，将通用云服务条款补充为能够履行、检查和追责的项目安排，并在服务期间持续验证相关安排的有效性。

### （一）合同应当明确责任、数据和服务要求

金融机构适用的监管要求，需要通过云服务合同进一步转化为服务商能够履行和金融机构能够检查的具体义务。通用云服务协议通常侧重产品功能、计费规则 and 标准服务水平，难以完整覆盖金融机构在数据管理、业务连续性、监管检查和退出安排等方面的要求。因此，金融机构需要结合上云系统、数据范围、服务模式和供应链结构，对标准协议进行补充。具体而言：

1. 云服务合同应当明确服务范围、交付内容和责任边界。金融机构可以根据实际架构，对云服务涉及的具体事项分别确定责任主体；在混合云或者多供应商模式下，还应明确不同服务商之间的责任边界。

**需要注意的是，服务商承担具体技术操作，并不相应转移金融机构依法承担的信息科技管理、网络安全和数据安全责任，金融机构仍应注意做好自身合规。**

2. 数据条款应当与数据清单和实际数据流向一致，明确数据类型、处理目的、存储地域、访问权限、保存期限以及返还或者删除方式。涉及分包或者转委托的，还应披露实际参与服务的主体，并根据事项重要程度设置通知、评估或者审批程序，确保数据保护、事件报告和退出处理等要求能够落实至相关参与方。

对于 MaaS 等模型服务，还需明确提示词、训练样本、模型输入输出和运行日志能否被服务商留存或者用于合同约定之外的用途。

3. 合同还应结合系统重要程度约定可用率、灾备和事件响应等要求。例如，《银行保险机构数据安全管理办法》要求银行保险机构在发生数据安全事件后两小时内向监管部门报告；《中国人民银行业务领域网络安全事件报告管理办法》对较大级别及以上网络安全事件规定了一小时内初步报告要求。由此，我们理解在设定服务商的事件通知时限的过程中，应当为金融机构开展事件研判、处置和履行监管报告义务预留必要时间，并要求服务商持续提供影响范围、处置进展和初步原因等信息，妥善保存相关日志和调查材料。

### （二）迁移和运行应当保持持续可控

金融机构上云迁移涉及数据、系统接口和运行环境变化的，应当事先明确迁移范围、实施窗口、职责分工、数据核验、备份和回退安排，并根据系统重要程度开展相应测试。正式投产前，应当完成缺陷整改、技术验证和项目验收，并履行适用的内部审议及监管程序。

系统投产后，金融机构仍需持续监测服务质量、服务商经营和安全状况、分包商服务情况以及集中

度风险。服务商调整系统架构、数据中心、服务地域、关键分包商或者数据处理方式的，应当要求其根据影响程度履行通知、评估、测试或者审批程序；相关变化触发金融机构适用的法定风险评估或者监管报告要求的，还应及时履行相应程序。

### （三）审计和退出安排应当能够实际执行

金融机构应当保留对云服务开展监测、检查和审计的权利，并要求服务商及相关分包商按照适用规则配合监管检查。非私有云等导致云环境无法直接开放全部底层资源的，亦可以结合项目风险采用独立审计报告、专项材料、联合检查或者受控验证等方式进行检查和监督。

此外，由于云项目退出涉及到金融机构数据迁移，因此我们建议，退出方案应当在采购和签约阶段确定，并在服务期间根据系统和供应链变化及时更新。相关安排应明确退出触发条件、过渡服务期限、迁移协助以及数据、日志、备份、配置和必要文档的导出和核验方式。完成迁移后，还应按照适用规则处理数据返还或者删除、账号和权限撤销以及资源释放；依法需要继续保存的数据和日志，应当明确保存依据、期限和后续安全管理责任。

## 五、结语

金融机构上云，转移的是部分技术资源和服务活动，不能随之转移的是机构自身的管理责任。

监管关注的重点并不因是否用了“云”而变化，金融机构上云项目可能同时涉及信息科技外包、重要信息系统投产和变更、数据委托处理、网络产品和服务采购以及业务连续性管理等既有的机构管理要求。故在使用云服务时，金融机构仍需从自身角度做好项目事实排查、合规要点梳理及合规要求落实，把握好效率与合规的平衡。

## 特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

### 权威

电话： +86 21 6080 0946

Email: [wei.quan@hankunlaw.com](mailto:wei.quan@hankunlaw.com)

### 朱俊

电话： +86 10 8525 4690

Email: [jun.zhu@hankunlaw.com](mailto:jun.zhu@hankunlaw.com)

### 李珣

电话： +86 21 6080 0232

Email: [xun.li@hankunlaw.com](mailto:xun.li@hankunlaw.com)

### 夏迎雨

电话： +86 21 6080 0963

Email: [yingyu.xia@hankunlaw.com](mailto:yingyu.xia@hankunlaw.com)