云计算开源产业联盟
OpenSource Cloud Alliance for industRy,OSCAR

可信金融云服务（银行类）能力要求参考指南（2018年）

云计算开源产业联盟

OpenSource Cloud Alliance for industry，OSCAR

2018年8月

版权声明

编写说明

牵头单位： 中国信息通信研究院

参与单位： 融联易云金融信息服务（北京）有限公司、兴业数字金融服务（上海）股份有限公司、招银云创（深圳）信息技术有限公司

编写人： 栗蔚、徐恩庆、董恩然、张春林、张世荣、陈翀、郑子洲、许志恒、侯大鹏、程剑豪、李荣杰、陈欣炜、张琳琳

前　言

数字化浪潮的来袭颠覆了整个金融行业，云计算、大数据、区块链等技术的普及，使得科技金融、互联网金融等全新金融业态迅速崛起。传统金融机构纷纷提出数字化战略，催生出对 IT 系统处理能力的更高要求，“银行上云”已是全行业的共识。

云计算为银行类金融机构快速部署银行业务系统提供了有力的信息化支撑，能够促进银行类金融机构提高信息化管理能力，有效增强业务竞争能力。同时，相对于普通企业，银行类金融机构业务需求、安全需求、政策符合性考虑等有明显的行业特色。

本指南研究银行类金融云服务的提供方在企业属性、服务协议、技术实力、服务保障、风险管理等方面的能力要求，在面向大众市场的可信云服务要求的基础上，提出可信金融云服务（银行类）的能力要求。银行业作为传统金融行业中对信息化技术和安全等方面要求最高的行业，可信金融云服务（银行业）能力要求同样也是最高等级的要求。本指南为银行上金融云选择可信的云服务提供依据，为面向银行类客户提供金融云服务的单位提供参考。

目 录

1. 可信金融云服务（银行类）基本概念

本指南所涉及的内容适用于银行用户在制定好上云策略[1]后，选择合适的云服务提供方和服务产品环节。

本指南所涉及的内容适用于以下定义的银行类金融云服务。

1.1 金融云服务（银行类）

金融云服务（银行类）或称银行类金融云服务指的是具有银行背景或属性的机构，向具有相同银行背景或属性的用户，提供满足银行业监管要求的云计算服务。

目前有两种模式的银行类金融云服务，一类是银行集团内部建设的面向本银行系统各级机构的金融云服务，另一类是其他银行或银行属性的公司输出的金融云服务。这两种模式的云服务在企业属性、风险管理、服务协议、技术实力、服务保障等方面都应达到可信金融云服务（银行类）级别的能力要求。

两种模式具体情况如下图：

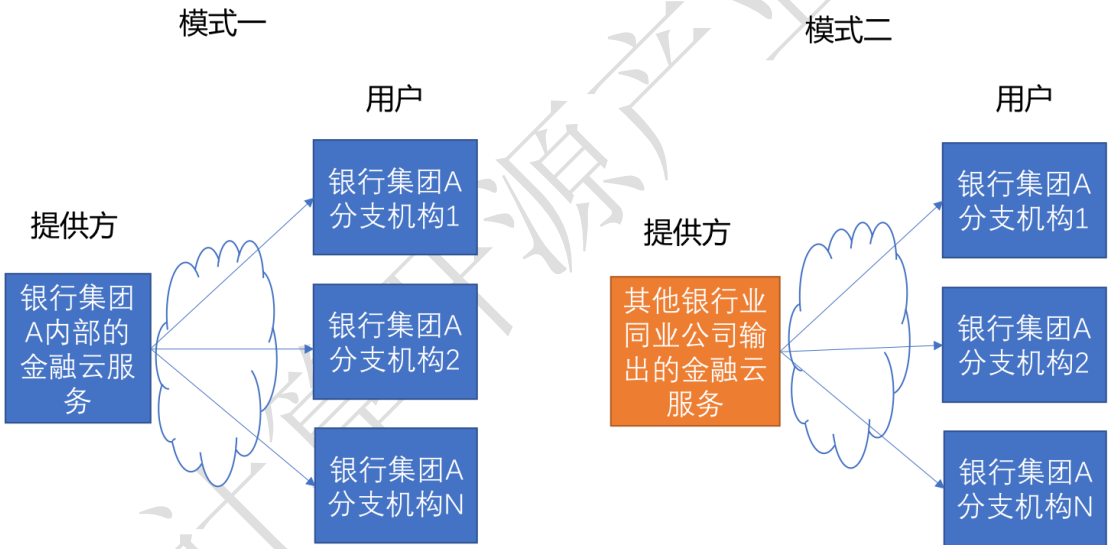

图 1 银行类金融云服务两类模式

用户：银行类金融云服务用户即银行系统中金融云服务（银行类）的使用者，可以是大中小银行，也可以是银行的分支机构；

提供方[2]：银行类金融云服务提供方即提供金融云服务能力的主体，模式一的提供方为和用户同属一个集团单位的内部机构，模式二的提供方为银行系统其他单位的主体，和用户不在一个集团单位。

用户和提供方都应具备银行业同业特征。

1.2 可信云服务

[1]银行用户上云决策框架参考附录 1

[2]提供方可以是具有独立法人的银行系统单位，也有可以是银行系统的某一个部门、事业部或机构

根据可信云系列标准，可信云服务梳理了云服务用户关心的16个基本指标，包括数据存储的持久性、数据可销毁性、数据可迁移性、数据私密性、数据知情权、服务可审查性；服务质量类：服务功能、服务可用性、服务资源调配能力、故障恢复能力、网络接入性能、服务计量准确性；权益保障类：服务变更和终止条款、服务赔偿条款、用户约束条款和服务商免责条款。可信云服务需要在以上16个指标方面做到可信，可信包括能力透明和能力真实，包括：

（1） 能力透明：16 个指标都已经通过服务协议向用户进行了承诺，且承诺的表述规范，简称：透明；

（2） 能力真实：16 个指标的真实能力能够达到承诺的水平，简称：真实。

1.3 可信金融云服务（银行类）

可信金融云服务（银行类）或称可信银行类金融云服务，将可信云服务的 16 个基本指标定义为基础可信指标，在基础可信指标基础上，进一步梳理归纳了银行云用户关心的服务保障和风险管理两类行业特性指标。最终将可信金融云服务（银行类）的指标归纳为五大能力方面，即企业属性、风险管理、服务协议、技术能力、服务保障五方面，这五方面可信要求包括：

（1） 能力透明：用户关心的能力指标都已经通过服务协议向用户进行了承诺，且承诺的表述规范，简称：透明；

（2） 能力真实：真实能力能够达到承诺的水平，简称：真实；

（3） 能力达标：达到银行级别金融云标准要求,简称：达标。

可信金融云服务（银行类）和普通可信云服务能力要求的差别，如下图。根据可信云系列标准[3]，普通的可信云服务能力要求为云服务在企业属性、服务协议和服务技术三方面做到透明和真实，只要云服务提供方的能力能够达到其服务协议承诺的水平即可，不需要达到具体的水平。而可信金融云（银行类）比普通可信云多了服务保障和风险管理两个能力方面，并且在透明和真实的基础上要求能力指标应达到具体的金融行业中最高要求的银行用户级别要求。比如，普通可信云的可用性承诺值和水平可以是 99.9%-99.99%区间的某个值，在本指南和可信金融云服务（银行类）相关标准中要求云服务提供方的能力和承诺都应达到 99.95%。

[3] 可信云系列标准:
《云计算服务协议参考框架》YDB 143-2014
《云计算服务客户信任体系能力要求 第 1 部分：云主机服务》
《云计算服务客户信任体系能力要求 第 2 部分：对象存储》
《云计算服务客户信任体系能力要求 第 3 部分：云数据库》
《云计算服务客户信任体系能力要求 第 4 部分：企业级 SaaS 服务》
《云计算服务客户信任体系能力要求 第 5 部分：块存储》
《云计算服务客户信任体系能力要求 第 6 部分：负载均衡》
《云计算服务客户信任体系能力要求 第 7 部分：物理云主机》

可信金融云服务（银行类）的五大能力方面三大可信要求，以及和普通可信云服务的关系具体如下：

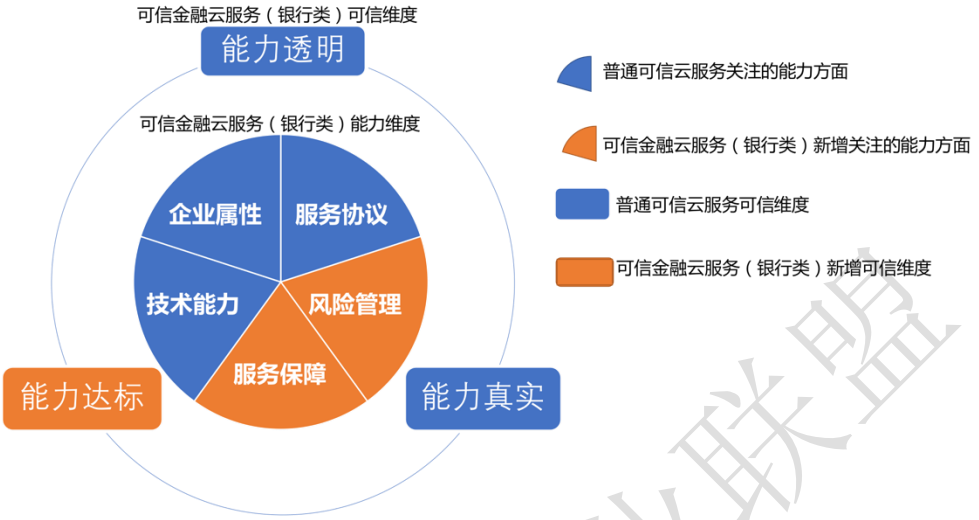

图 2 可信金融云服务（银行类）能力维度

（1） 企业属性可信要求，指的是提供方的背景符合同业特征和监管要求；参考本指南第 3 章及附录 2；

（2） 风险管理可信要求，指的是提供方在 IT 服务、信息安全、开发测试、业务连续性和科技外包等几个方面的风险管理能力要求。具体参考本指南第 4 章及附录 3。

（3） 服务协议可信要求，指的是提供方向用户提供的服务协议符合条款完备性和规范性要求，提供方是否就用户关心的所有指标和条款进行了承诺或说明，需承诺或说明的条款完备性和规范性参考本指南第 5 章及附录 4。

（4） 技术能力可信要求，指的是提供方云服务的数据安全、服务质量、性能三大方面达到银行类金融云服务的要求，具体内容参考本指南第 6 章及附录 5、附录 6 和附录 7。

（5） 服务保障可信要求，指的是提供方在运营监控、技术支持、服务报告、服务评价和服务改进等几大方面的可信要求。具体参考本指南第 6 章及附录 5、附录 6 和附录 7。

2. 可信金融云服务（银行类）应用场景及产品框架

2.1 银行对信息科技系统的新需求

在新一代金融科技技术和互联网的影响下，银行对传统的信息技术系统有新的需求，包括支撑突发的海量交易；应用快速开发迭代；快速开业、降低信息系统成本和运维复杂度等。

2.1.1 支撑突发的海量交易

由于互联网的发展，网上交易量在某些特定时间，无法准确预测峰值，需要银行信息科技系统支持快速的资源弹性扩展，满足突发海量交易的需求。

2.1.2 应用快速开发迭代

互联网金融产品层出不穷，各种金融应用产品开发、上线、迭代越来越快，需要信息科技系统支持分布式的应用开发场景，满足应用快速开发迭代。

2.1.3 快速开业、降低信息系统成本和运维复杂度

出于运营成本的考虑，采用按需采购云服务的模式，银行发展信息科技面临的财力、人力压力可以得到极大减轻。同时，银行无需再配备 IT 方面的专业运维人员，从最大程度上使其可以集中投入发展核心业务。

2.1.4 优化灾备策略

信息科技系统灾备建设对银行来说至关重要，必须要有一个可靠的容灾系统在灾难到来时保障业务不间断运行，传统灾备建设存在 IT 设备资源率较低、维护成本高等问题。随着信息技术的发展，灾备云技术可以为银行建设灾备中心提供新的策略。

2.2 银行云服务应用场景

面对以上银行对云信息科技系统的新需求，银行云服务可以实现资源弹性扩展、支持分布式应用开发测试平台、支持银行系统托管、灾备等应用场景，满足银行新的信息技术系统需求。较之普通公有云服务提供方,从事银行云服务的服务提供方应获得相关监管机构的认可，并且定期接受监管机构的监督检查。

2.2.1 资源弹性扩展

银行云服务提供计算、存储、网络等IaaS基础资源服务，可以为银行在开展高峰交易量的业务时，短时间内购买云服务的基础资源，来支撑海量突发交易量。

例：在双十一等促销活动日到来时，银行交易量远大于平时，交易系统对基础资源的要求也随之剧增，银行云服务可以应对资源弹性扩展的需求。

2.2.2 分布式应用开发测试平台

银行云服务提供分布式应用开发和托管的PaaS服务，满足银行应用快速开发迭代的需求。

2.2.3 银行系统托管

银行云服务提供IaaS和PaaS，银行使用银行云服务托管已有业务系统或直接使用银行业务SaaS。银行云服务为银行快速开业、降低信息系统成本和运维复杂度提供支持。

2.2.4 灾备

银行云服务提供灾备云服务，提供可靠的容灾系统保障银行信息科技系统稳定运行。

2.3 可信金融云服务（银行类）产品框架

2.3.1 银行业云服务产品框架

为了满足以上银行云服务计算的需求，银行云服务主要提供基础设施即服务IaaS、平台即服务PaaS和软件即服务SaaS三类云服务，不同的云服务提供方提供其中的一种、几种或全部云服务，银行客户可自行选定服务组合。具体情况参见附录2。

图 3 银行云服务产品框架

2.3.2 基础设施即服务（IaaS）

在IaaS模式下，云服务提供方向用户提供虚拟计算机、存储、网络等计算资源，提供访问云基础设施的服务接口。用户可在这些资源上部署或运行操作系统、中间件、数据库和应用软件等。用户通常不能管理或控制云基础设施，但能控制自己部署的操作系统、存储和应用，也能部分控制使用的网络组件。

2.3.3 平台即服务（PaaS）

在PaaS模式下，云服务提供方向用户提供的是运行在云基础设施之上的软件开发和运行平台，如：标准语言与工具、数据访问、通用接口等。用户可利用该平台开发和部署自己的软件。用户通常不能管理或控制支撑平台运行所需的底层资源，如网络、服务器、操作系统、存储等，但可对应用的运行环境进行配置，控制自己部署的应用。银行云服务PaaS服务主要包括开发测试、持续集成持续交付、微服务。

2.3.4 软件即服务（SaaS）

在 SaaS 模式下，云服务提供方向用户提供的是运行在云基础设施之上的应用软件。用户不需要购买、开发软件，可利用不同设备上的用户端（如 WEB 浏览器）或程序接口通过网络访问和使用云服务提供方提供的应用软件。银行 SaaS 服务主要包括核心银行类、渠道服务类、专用产品和服务类、风险管理类、客户关系管理类、基础平台类、网关类、支持功能类、管理信息类。

3.可信金融云服务（银行类）提供方企业属性

可信金融云服务（银行类）提供方企业属性需和用户同一属性，即银行属性，且其所有用户也应同属银行属性，具体如下：

1) 内部云服务提供方企业属性

——具备信息安全管理体系评估认证，具有健全的组织架构、有效的风险治理架构和专职的信息科技风险管理团队，定期开展风险评估和审计工作；

——具备与所承担的服务范围和业务规模相适应的服务管理体系；

——具有足够的技术能力、人力资源和设施、环境，满足云计算服务的质量和安全管理要求；

——支持内部结算等支付方式。

2) 外部云服务提供方企业属性

——如提供IaaS或PaaS服务，应具有IDC（含互联网资源协作服务）经营许可证；

——应提供公司企业法人营业执照、公司整体社保缴纳信息证明和组织机构证书；

——应为银行机构或由其控股的科技公司；

——应提供连续两年向监管机构报送的证明；

——有ICP、ISP或第三方支付等行业部门颁发的相关牌照；

——具有连续纳税证明材料；

——具有验资报告；

——应具备一定的运营规模，银行用户数达到10家以上，或物理CPU颗数120个以上，或虚拟CPU核数240核以上；

——应提供业务基本信息：

- 业务名称；
- 业务运营起始时间；
- 业务功能；
- 支付方式；
- 业务采用的软件、硬件。

4. 可信金融云服务（银行类）风险管理可信要求

银行用户应做好对云服务提供方的监督管理，建议参考中国信息通信研究院牵头制定的《可信金融云服务（银行类） 第2部分：风险管理能力要求》，从IT服务管理、信息安全管理、开发测试管理、业务连续性管理和科技外包管理等方面明确具体管理要求，防范运行风险。

银行云服务提供方应建立有效信息科技风险管理体系，具体要求包括但不限于：

- 银行云服务平台和银行业重要信息系统应具备符合公安部信息安全等级保护三级或者更高级的指标能力要求；
- 应符合 ISO 20000 IT 服务管理体系的管理能力要求；
- 应符合 ISO 27001 信息安全管理体系的管理能力要求；
- 应符合工业和信息化部的可信云服务指标的能力要求；
- 应符合工业和信息化部的云计算风险管理框架相关指标的能力要求；
- 应至少连续两年稳定运行（可用性达标），并向相关监管机构连续两年报送持续运行情况
- 应遵守国家相应的法律法规，配合银行、银行监管机构及派出机构的监管审查。

详见附录3。

5. 可信金融云服务（银行类）服务协议能力要求

银行需确保与云服务提供方签订规范的服务合同，将有助于保证服务质量，便于上云后的管理。云服务提供方和客户应就所使用的云服务签订标准的合同及服务协议，就云服务提供的标准、质量、风险等达成共同的约定。建议参考中国信息通信研究院牵头制定的《可信金融云服务（银行类） 第3部分：服务协议参考框架》，拟定银行类云服务协议的框架和关键项。

服务协议一般包括三个部分：

一、合同主体，包括：约定的服务范围、甲乙方双方权利、服务收费和付款、合同的变更终止和解除、知识产权的声明、违约情况、不可抗力以及其他法律约定的合同必备内容。

二、服务级别协议SLA，包括：服务目录、服务可用性的承诺和细项说明、服务质量保证的方法、服务考核和质量考核、服务评价等。

三、保密协议，服务甲乙双方宜签订单独的保密协议，用以明确甲乙双方就一方（“披露方”）向另一方（“接受方”）披露的秘密信息所应承担的保密义务，包括：保密责任、保密期限、免责条款、违约责任、协议的效力变更和终止等。

服务协议一般包括云服务功能、云服务可用性条款、数据安全类条款、云服务质量类条款、质量保障类条款、权益保障类条款。

详见附录4。

6. 可信金融云服务（银行类）技术和服务能力要求

可信金融云服务（银行类）应满足行业主管部门的相关要求指引，包括但不限于：

- 《银行业信息系统灾难恢复管理规范》（JR/T 0044—2008）
- 《网上银行系统信息安全通用规范》（JR/T 0068—2012）
- 《金融行业信息系统信息安全等级保护实施指引》（JR/T 0071-2012）
- 《金融行业信息系统信息安全等级保护测评指南》（JR/T 0072-2012）
- 《金融行业信息安全等级保护测评服务安全指引》（JR/T 0073-2012）
- 《中小银行银行信息系统托管维护服务规范》（JR/T 0140—2017）
- 《网络安全等级保护条例》（征求意见稿）
- 《中小金融机构灾备云技术规范》（征求意见稿）
- 《中小金融机构灾备云安全要求》（征求意见稿）
- 《中小金融机构灾备云服务管理规范》（征求意见稿）
- 《中国银监会关于印发商业银行信息科技风险管理指引的通知》（银监发[2009]19号）
- 《中国银监会关于印发商业银行业务连续性监管指引的通知》（银监发[2011]104 号）
- 《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》（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）

市面上的云服务提供方服务能力参差不齐，如何评估云服务的技术和服务能力成为银行类金融机构在选型云服务时面临的一大关键问题。针对此问题，中国信息通信研究院牵头制定的《可信金融云服务（银行类） 第4部分：基础设施即服务技术和服务能力要求》、《可信金融云服务（银行类） 第5部分：平台即服务技术和服务能力要求》、《可信金融云服务（银行类） 第6部分：软件即服务技术和服务能力要求》分别对银行类云服务的IaaS、PaaS和SaaS产品提出了具体的技术和服务能力要求。

银行客户在选型具体云服务时可参考上述标准，自行或委托相关机构对云服务进行评估，将评估结果作为确定云服务提供方的重要参考依据。

具体详见附录5、附录6和附录7。

附录 1：银行客户上云决策框架

1. 银行客户上云决策框架整体思路

在传统的信息化建设模式下，银行直接投资构建 IT 设施、服务器以及网络，拥有信息化资源的所有权；现在，需要转换思维，把 IT 看作服务，看作是商品化的计算资源和服务。这种全新的思维方式对整个 IT 服务的生命周期都产生了重大影响。

本指南提出了银行上云的决策框架，从上云前准备、上云实施到上云后管理三个流程提出决策建议。供计划实施上云的有关银行类金融机构参考。

表 1 银行上云决策框架

上云前准备	上云实施	上云后管理
● 确定上云优先级和可行性方案 ● 选择合适的云服务提供方和产品	● 服务合同制定和签署 ● 服务提供方案设计和测试 ● 服务交付	● 服务质量监督管理 ● 风险管理 ● 变更和退出

2. 银行上云前准备

2.1 确定上云优先级

确定上云优先级是银行上云的第一步工作，也是最重要的工作。银行在上云之前应全面审视自己的业务系统，认真评估其 IT 资产，仔细设计路线图，将适合云化部署且准备比较充分的服务置于首选地位，以使上云带来的收益最大化、成本最小化。

银行因资产规模区别，业务系统种类和数量一般也存在较大差异，资产规模较大的股份制商业银行和城市商业银行业务系统通常比较丰富，而银行中资产规模最小的村镇银行因盈利能力较弱系统较少。

银行业信息系统一般如下图所示：

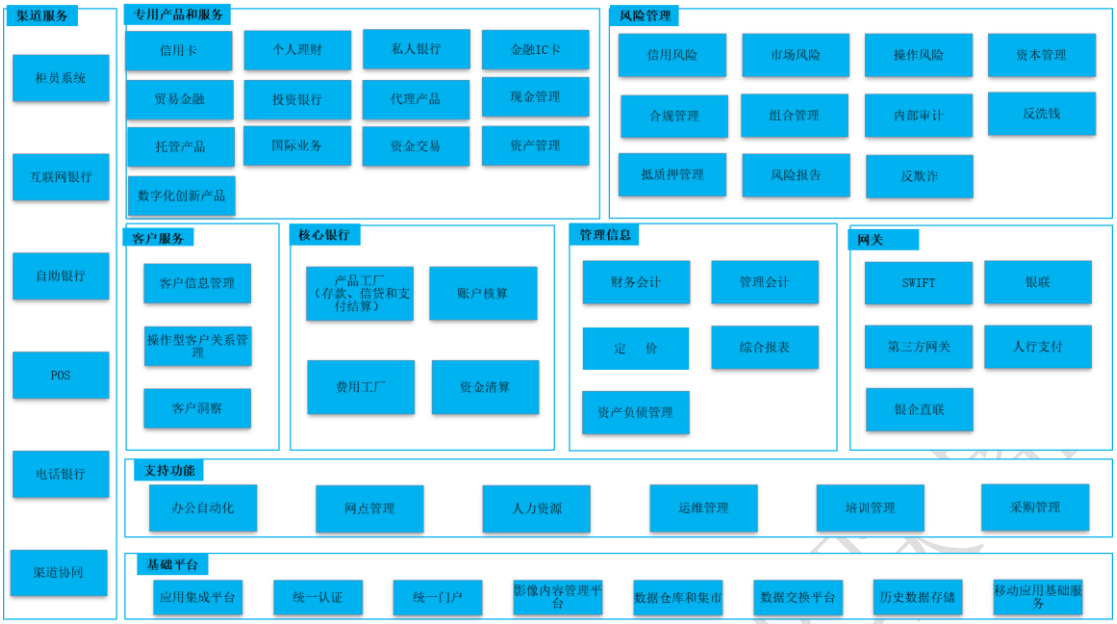

图 4 银行业信息系统

成本收益比、安全保护要求、监管机构管理要求、应用系统上云难度是确定业务系统上云优先级的主要考量因素。通常来说，确定上云优先级有几个参考原则。

一是对于需新部署的业务系统，且云服务提供方已有与之相对应的比较成熟的业务，从价值收益的角度建议不分业务类型，都首选云服务；

二是已有信息化系统，上云后价值效益明显的，也建议尽快上云，尤其像访问流量有突发变化特征或对数据融合处理有较高要求的系统，上云后能够带来明显的效益提升；

三是对于已有信息化系统，按照非核心系统和核心系统的区分确定优先级，先上非核心系统，后上核心系统。

2.2 选择合适的云服务提供方和产品

银行应根据业务需求和自身基础，从基础设施、平台系统、业务应用等方面合理选择云服务产品。银行在选择云服务提供方时应充分考察云服务提供方的资质、技术和服务能力，选择能够达到相应要求的云服务提供方。

2.2.1 资质考察

云服务提供方应具备各级主管部门颁发的运营资质，具备良好的信用等级，拥有协助企业上云的成功案例。对银行云服务提供方，建议满足下列要求：

- 银行云服务平台和银行业重要信息系统应具备符合公安部信息安全等级保护三级或者更高级的指标能力要求；
- 应符合 ISO 20000 IT 服务管理体系的管理能力要求；
- 应符合 ISO 27001 信息安全管理体系的管理能力要求；
- 应符合可信云服务指标的能力要求；
- 应符合云计算风险管理框架相关指标的能力要求；

- 应获得相关监管机构的认可，并且定期接受监管机构的监督检查。

2.2.2 技术和服务能力评估

如今市面上的云服务提供方形形色色，服务能力参差不齐，如何评估云服务的技术和服务能力成为银行类金融机构在选型云服务时面临的一大关键问题。

针对此问题，中国信息通信研究院牵头制定的**《可信金融云服务（银行类） 第 4 部分：基础设施即服务技术和服务能力要求》**、**《可信金融云服务（银行类） 第 5 部分：平台即服务技术和服务能力要求》**、**《可信金融云服务（银行类） 第 6 部分：软件即服务技术和服务能力要求》**分别对银行类云服务的 IaaS、PaaS 和 SaaS 产品提出了具体的技术和服务能力要求。

银行客户在选型具体云服务时可参考上述标准，自行或委托相关机构对云服务进行评估，将评估结果作为确定云服务提供方的重要参考依据。

3. 银行上云实施

3.1 服务合同制定和签署

银行需确保与云服务提供方签订规范的服务合同，将有助于保证服务质量，便于上云后的管理。

建议参考中国信息通信研究院牵头制定的**《可信金融云服务（银行类） 第 3 部分：服务协议参考框架》**，拟定银行类云服务协议的框架和关键项。

服务协议一般包括三个部分：

一、合同主体，包括：约定的服务范围、甲乙方双方权利、服务收费和付款、合同的变更终止和解除、知识产权的声明、违约情况、不可抗力以及其他法律约定的合同必备内容。

二、服务级别协议 SLA，包括：服务目录、服务可用性的承诺和细项说明、服务质量保证的方法、服务考核和质量考核、服务评价等。

三、保密协议，服务甲乙双方宜签订单独的保密协议，用以明确甲乙双方就一方（“披露方”）向另一方（“接受方”）披露的秘密信息所应承担的保密义务，包括：保密责任、保密期限、免责条款、违约责任、协议的效力变更和终止等。

3.2 服务提供方案设计和测试

3.2.1 方案设计

云服务提供方应依据云服务目标和服务级别协议进行云服务提供方案的设计，服务提供方案应涉及与云服务相关的资源配备、人力配备和管理要求。管理要求应涵盖组织管理、范围管理、质量管理、沟通管理、时间管理、风险管理、财务预算管理、技术管理、文档管理及其他资源管理，也应涉及测试验证流程、技术实施流程、服务交付流程、日常维护流程、应急处置与灾难恢复流程、验收考核流程等各个方面。

需要特别强调的是，除上线新业务外，很大部分工作在于存量业务应用的迁移，如何有序、安全、便捷地进行迁移，保证业务的可用性、安全性、连续性是必须考虑的重要环节。

服务提供方应按照前述附录 1 第 1 部分确定上云优先级及可行性方案的内容，针对不同的银行业务系统现状规划方案，包括：

（1）业务系统迁移的优先级及可行性方案;

（2）相应业务系统的资源使用规划和架构，包括计算、存储、网络等;

（3）相应的业务系统的运维管理模式，服务提供方和银行的权责划分等。

3.2.2 方案测试

云服务提供方在服务资源、人员和管理方面准备就绪后应测试并验证服务提供方案的完备性。测试和验证应满足以下要求：

（1）为避免云服务存在技术和管理方面的缺陷，云服务提供方应依据服务提供方案的内容对相关的技术手段、软件、设备和工具的可用性及性能、管理制度和流程的合理性等方面进行必要的测试及验证。

（2）云服务提供方应在测试验证前向银行用户提交测试验证方案，明确测试验证的方式、人员、环境、标准、文档等，银行用户应对测试验证方案进行评审。

（3）云服务提供方应按测试验证方案的内容向银行用户提供测试人员、准备测试环境、记录测试数据、提供测试报告，银行用户应提供必要的协助，并对测试验证报告的结果进行验证。

3.3 服务交付

3.3.1 交付方案

云服务提供方向银行用户提交详细的服务交付方案，包括服务交付时间、交付方式、交付人员、交付技术手段、交付文档、交付培训、交付验收标准和流程等，银行用户应对服务交付方案进行评审并与云服务提供方达成一致。

3.3.2 交付实施

银行用户应对云服务提供方提交的服务管理计划进行评审，并在服务交付过程中对云服务提供方的交付过程进行监督和检查，发现交付过程中存在问题和偏差时，应及时向云服务提供方反映，并要求云服务提供方采取必要的措施。在业务迁移的实施过程中，尽量应做到无停机的数据迁移，实现在线不停业务迁移；按照灵活部署原则，先迁移后择时割接。

3.3.3 交付评估

服务交付完成后，云服务提供方应向银行提交服务交付报告，银行可以组织第三方对迁移后的业务和云平台进行评估验收。详细记录服务交付的关键信息，如工作任务、所需资源、进展状态、负责和参与人员、完成时间、存在的问题、解决方案等，银行应组织相关人员对报告进行评审，通过后上线。

4. 银行上云后管理

4.1 服务质量监督管理

上云成功后，云服务提供方接受银行用户或受委托的第三方机构对云服务的监督和管理。云服务提供方和银行用户共同建立故障响应流程以及日常巡检、服务质量监督制度，督促云服务提供方为银行用户提供可靠的运行服务保障，推动服务质量持续改进。银行用户根据自身审计能力可以选择通过自行审计或委托第三方机构审计的方式，开展周期性评估审计。

银行用户管理云系统需要将云服务提供方、审计者和最终用户都考虑进来，将关注的侧重点聚焦于服务而非资产。需要有效地管理云服务提供方的输出过程(例如 SLA）而不是用户的输入过程(例如服务器的数量)。对出现的服务不可用或其他应对用户进行赔偿的场景，云服务提供方应按照与银行用户服务协议中约定的内容和方式，进行有效赔付，保证银行用户的合法权益。

4.2 风险管理

4.2.1 责任分担模型

银行用户必须加强防范云计算模式下的 IT 风险,保障业务信息和运行安全。银行在使用云服务的过程中，会有多种云计算技术的选择方式，同时也可能会面临多个云服务提供方。任何一个云服务的参与者都应当承担起相应的职责，不同角色的参与者通常会承担实施和管理不同部分的责任。云安全和云风险的职责会由参与者共同分担。建议的责任分担模型如下图所示：

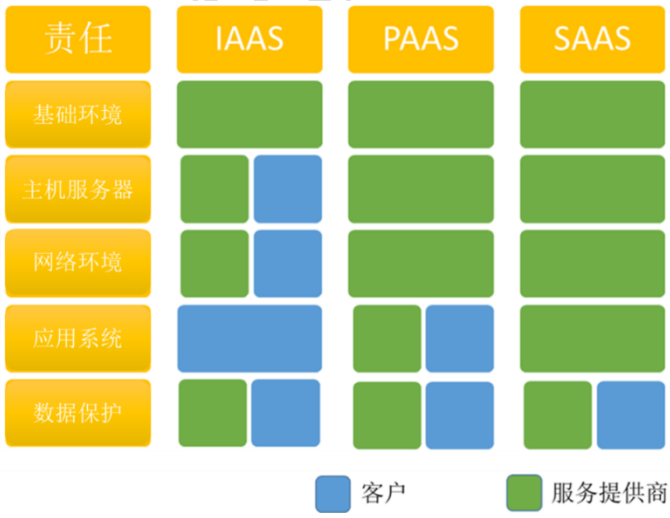

图 5 银行用户和服务提供方责任分担模型

在 IaaS 模式中，云资源使用方和云服务提供方共同保证主机服务器及网络环境的稳定运行。云资源使用方主要负责：提交云资源配置需求并正常使用云服务提供方提供的云主机、网络、安全策略等；按照本公司的风险管理要求进行云服务器和网络的变更，避免人为失误或方案疏忽等因素造成影响单个应用或整个云平台的风险事件。云服务提供方主要负责：按照云资源使用方的要求提供相应的云主机、网络、安全资源；负责维护整个云平台的高可用

运行，负责确保单个云主机或者单个物理机的故障能够自动、快速、有效恢复正常；负责在出现风险事件时，配合客户进行基础环境、主机环境、网络环境、甚至应用层面的故障排查、处置和恢复。

数据资产的安全和保护贯彻数据使用生命周期的各个环节，需要云资源使用方和云服务提供方共同维护、协同保障。2018 年 3 月 16 日，中国银监会发布了《银行业金融机构数据治理指引》（征求意见稿），要求银行业金融机构将数据治理纳入公司治理范畴，并将数据治理情况与公司治理评价和监管评级挂钩。明确鼓励银行业金融机构开展制度性探索，在公司设置首席数据官。强调银行业金融机构应顺应大数据时代的需要，同时所有相关方均应强化数据安全意识，依法合规采集数据，防止过度采集、滥用数据，切实依法保护客户数据安全。

4.2.2 自身风险管理“三道防线”

银行用户从自身来说，应制定完善的风险管理和安全保障制度，依据监管要求的“三道防线”的思路下设计整信息科技部门的风险管理体系架构，包括信息科技管理、信息科技风险管理和信息科技审计管理。重点做好数据风险管理，建立人才培养和技能储备机制，强化主动管理风险能力。

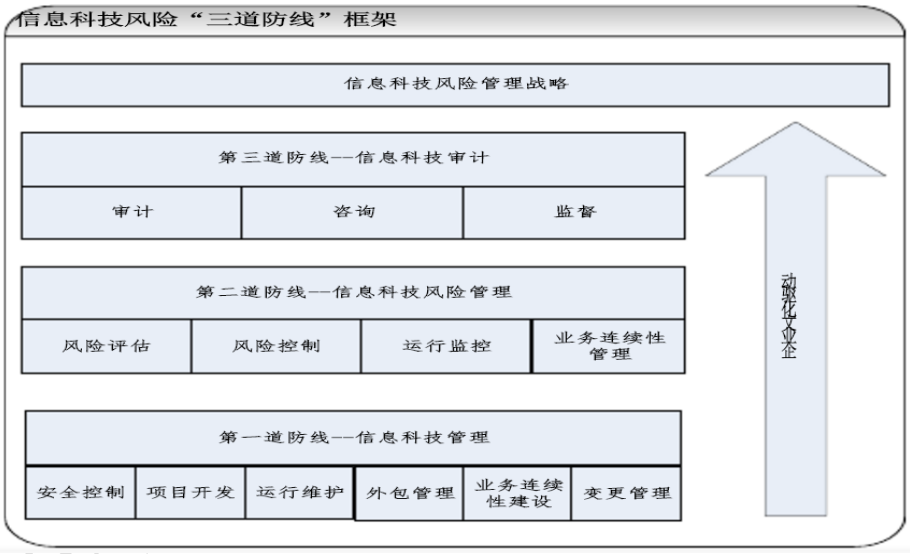

图 6 银行 IT 风险管理“三道防线”架构

4.2.3 对云服务提供方风险管理要求

银行用户应做好对云服务提供方的监督管理，建议参考中国信息通信研究院牵头制定的**《可信金融云服务（银行类） 第 2 部分：风险管理能力要求》**，从 IT 服务管理、信息安全管理、开发测试管理、业务连续性管理和科技外包管理等方面明确具体管理要求，防范运行风险。

4.3 变更和退出

4.3.1 服务变更

银行上云后由于业务变化会经常变更服务需求。银行用户发起服务变更请求，云服务提供方应及时响应，制定变更服务提供方案、实施计划和恢复方案；提出服务内容相匹配的服务内容说明及服务级别承诺；提出明确的时间计划，并与银行用户充分协商，审核确认，变更实施应避开银行业务运行敏感时间窗口。

4.3.2 服务退出

云服务由于情况变化、服务到期等原因中止或取消服务称为服务退出，服务退出可分为到期退出和提前退出。服务的退出应满足以下要求：

（1）在服务协议/合同到期前，银行用户应以书面方式明确退出服务协议/合同，云服务提供方应及时响应，并共同细化服务退出方案，包括但不限于退出实施计划和资源处置方案。

（2）需提前退出服务的，提出退出的机构应说明服务退出的理由，提出服务退出和过渡方案，并为双方协商和云服务的平稳过渡预留足够时间。

（3）云服务提供方应协助银行用户，在服务退出过程中，保证业务系统的有效运行和数据完整。

5. 参考政策文件及标准

支持云计算发展的政策相继出台，政策环境持续利好。近年来，国内云计算发展政策集中出台，我国云计算产业发展、行业推广、应用基础等重要环节的宏观政策环境已经基本形成。国家层面相继出台以下政策文件和标准：

- 2015 年 1 月，《国务院关于促进云计算创新发展培育信息产业新业态的意见》（国发〔2015〕5 号）
- 2015 年 5 月，《关于加强党政部门云计算服务网络安全管理的意见》
- 2015 年 7 月，《国务院关于积极推进“互联网+”行动的指导意见》
- 2015 年 8 月，《促进大数据发展行动纲要》（国发(2015)50 号）
- 2017 年 3 月，《云计算发展三年行动计划（2017-2019 年）》
- 《云计算服务客户信任体系能力要求 第 1 部分：云主机服务》
- 《云计算服务客户信任体系能力要求 第 2 部分：对象存储》
- 《云计算服务客户信任体系能力要求 第 3 部分：云数据库》
- 《云计算服务客户信任体系能力要求 第 4 部分：企业级 SaaS 服务》
- 《云计算服务客户信任体系能力要求 第 5 部分：块存储》
- 《云计算服务客户信任体系能力要求 第 6 部分：负载均衡》
- 《云计算服务客户信任体系能力要求 第 7 部分：物理云主机》

附录 2：可信金融云服务（银行类） 第 1 部分: 场景需求与总体框架

附录 3：可信金融云服务（银行类） 第 2 部分：风险管理能力要求

附录 4：可信金融云服务（银行类） 第 3 部分：服务协议参考框架

附录 5：可信金融云服务（银行类） 第 4 部分：基础设施即服务技术和服务能力要求

附录 6：可信金融云服务（银行类） 第 5 部分：平台即服务技术和服务能力要求

附录 7：可信金融云服务（银行类） 第 6 部分：软件即服务技术和服务能力要求

附录 2-附录 7 中具体内容请咨询中国信息通信研究院云大所云计算部门。

联系人：董恩然

电话：18601280900