【解读】中小银行信息系统托管维护服务规范

2017 年 2 月 14 日中国人民银行正式发布了金融业行业规范《中小银行信息系统托管维护服务规范》JR/T 0140-2017。

适用对象

3.1

中小银行 small and medium bank

依法设立的股份制商业银行、城市商业银行、农村商业银行、农村合作银行、村镇银行等，其中股份制商业银行不包括国有大型股份制商业银行。

从发文对象和定义来看，基本上除了五大行，工农中建交，其他都属于中小银行。

这有点像数据中心的分类，小于 3000 机柜都属于中小型数据中心。

国家层面看大部分一般都定义成中小型。大型和超大型一般都是有一点平等对话权的。

当然并不是说大型银行，就不能将信息系统服务进行托管，只是他们将有专门的大型银行信息系统托管维护服务规范。

IT 基础设施与架构的区别

3.14

IT 基础设施 IT facility

包含机房空间、动力、环境控制等IT设备及应用运行所必需的基础环境。

3.15

IT 基础架构 IT infrastructure

包含服务器、存储、网络、操作系统、中间件和数据库等IT应用运行所必需的基础硬件及软件环境。

虽然名字不是很对称，比如

IT 基础设施或许叫基础设施或者 DC facility 更恰当点；

而 IT 基础架构如果指 infrastructure，一般云计算的常规定义中是指包含服务器、存储、网络等 IT 上层应用所必须的基础硬件。

不过规范既然这么规定了，我们这么理解就成。

服务类型与范围

4.2 托管维护服务范围和类型

委托机构可将除IT管理责任之外的其他IT服务，包括：基础设施、基础架构、应用系统和数据等有选择地托管于受托机构的物理场所。托管维护服务根据托管服务内容的不同主要可分为以下三种类型：

a) 基础设施级托管：受托机构提供数据中心基础设施运维服务，IT 基础架构、应用系统和数据的运维都由委托机构负责。

b) 基础架构级托管：受托机构提供数据中心基础设施和 IT 基础架构的运维服务，应用系统和数据的运维都由委托机构负责。

c) 应用系统级托管：受托机构提供数据中心基础设施、IT 基础架构、应用系统和数据的运维服务。

托管维护服务的范围和类型如图1所示：

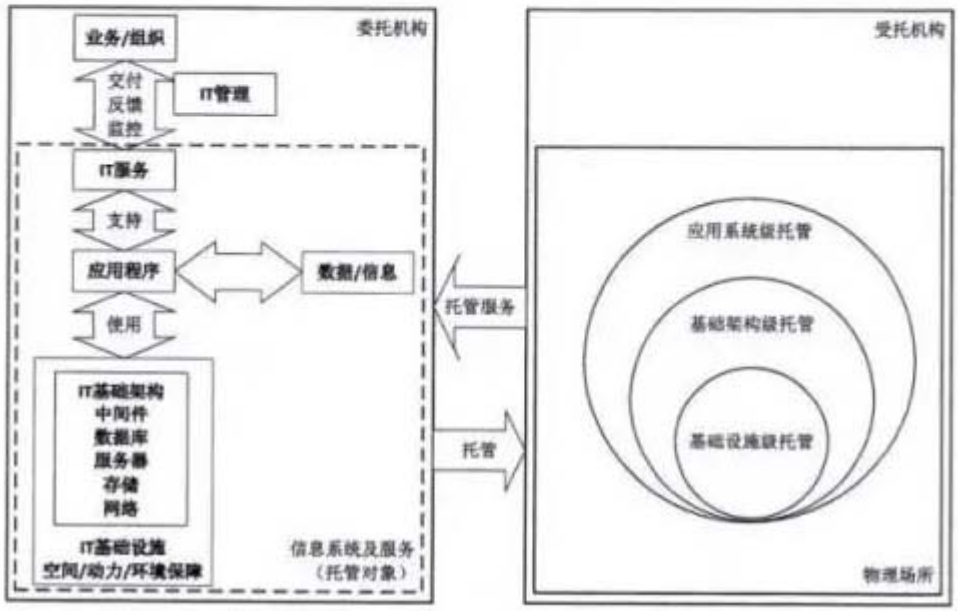

图1 托管维护服务范围和类型的示意图

套用云计算的叫法：

基础设施级托管：FAAS，facility as a service；与 IAAS 的区别，在于不提供服务器，只提供服务器的运行物理环境（风火水电）的托管和服务。就像典型 IDC 服务器托管服务一样，只是针对的客户是银行业，因其特殊性和重要性，而需要满足特定的监管和规范要求，比如本规范。

基础架构级托管 :介于常规 IAAS(基础设施即服务)与 PAAS(平台即服务)之间 ,甚至是 PAAS 与 SAAS（软件/应用即服务）之间。

应用系统级托管：SAAS。原以为银行应该不可能做成 SAAS，不过目前看来这扇门并没有关闭，是因为互联网金融么？

从这些原则来看 CAAS(通讯即服务),MAAS(物联网即服务 ,未来的无人值守应该需要建立在 MAAS

基础之上）在银行业也存在一定成长空间。

中小银行推荐关注

5.1.1 委托机构的组织原则

委托机构的组织原则如下：

a) 委托机构应承担信息科技管理职能，信息科技管理责任不能外包。

b) 委托机构应对托管维护管理中的不同角色有明确分工和职责定义。

c) 委托机构的岗位设置应按照“关键岗位不兼容”的原则，不兼容岗位之间禁止出现互相兼职的情况。

5.1.3 委托机构管理职能的实现

b) 委托机构应遵循“关键岗位不兼容”原则明确关键岗位的范围，确定不可相互兼职的岗位要求，至少应保证服务内容的管理、服务机构的管理、审计和评估的管理由不同部门、岗位或人员分别承担。

6.2 服务需求的评估

为明确服务需求，委托机构和受托机构应开展如下工作：

a) 委托机构应首先对自身托管服务的必要性、重要性和紧迫性进行充分地评估，并向受托机构明确托管服务的服务目标、内容、范围、规模、方式，以保证托管服务符合委托机构的业务战略、满足委托机构的信息系统运行环境要求。

c) 委托机构应对托管服务和受托机构可能引入的风险进行充分的分析和评估，根据风险评估的结果制定有效的风险管控策略和风险处置措施，以避免对委托机构业务产生不利影响。风险评估的结果应形成书面的风险评估报告，必要时可委托第三方专业机构对托管服务和受托机构进行专项风险评估工作。

7.5 服务方案的测试验证

受托机构在服务容源、人员和管理方面准备就绪后应测试并验证服务方案的完备性。

8.1.3 重大事件的处置

f) 受托机构有责任配合委托机构对重大事件开展独立或委托第三方调查。

g) 委托机构可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。

h) 情节特别严重的，委托机构可考虑取消受托机构服务准入资质，并报监管机构申请对其备案。

8.2.2 监控和巡检管理

b) 应采取人工值守和自动化工具相结合的方式，对重要信息系统进行 7×24 小时实时监控。

i) 应定期评估监控系统设计与执行的有效性，持续满足运维要求。

8.4.1 风险管理

e) 受托机构应对所有员工进行必要的培训，使其充分掌握信息科技风险管理制度和流程，了解违反规定的后果，并对违反安全规定的行为采取零容忍政策。

f) 委托机构为避免供应商依赖以及核心能力丧失的风险，应建立人才和技能储备机制，受托机构应予以配合。

g) 委托机构进行风险评估时，受托机构应予以配合，并提供相关材料。

9.1.3 突发性变更及终止服务

b) 委托机构应按照事先准备的服务中断应急预案处置。

10.1.2 内审频率的要求

受托机构应根据托管服务的性质、规模和复杂程度，关键业务影响情况，以及信息科技风险评估结果，决定内部审计范围和频率，至少应每三年进行一次全面审计。涉及关键业务或关键系统的应每年开展一次全面审计。

10.3 独立第三方审计

a) 外部审计机构根据授权出具的审计报告，经审计内容涉及的相关监管机构审阅批准后具有与相关监管机构出具的检查报告同等的效力，受托机构或委托机构应根据该审计报告提出整改计划，并在规定的时间内实施整改。

托管并不是将责任移交出去，中小银行作为真正系统拥有和运营者，相关的责任是不可推卸的，尤其

是面对监管层所关心的。

以上仅是笔者个人的关注角度，还请详细阅读各省市人民银行下发的规范全文。

托管服务商推荐关注

5.3.1 受托机构应具备的资质

受托机构应根据托管服务内容建立服务质量标准，并具备相应的服务资质，如下：

a) 受托机构应具有完善的IT服务管理体系、信息安全管理体系、业务连续性管理体系，应获取金融行业公认较为权威的管理资质认证。

b) 重点受托机构应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2000万元，向银行业金融机构持续提供信息系统托管维护服务的时间应不少于3年。

c) 重点受托机构应拥有健全的组织架构和有效的信息科技风险管理体系，建立由受托机构高级管理层直接领导、针对托管服务的专职信息科技风险管理团队，为托管服务安全提供保证。

d) 重点受托机构应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、服务连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。

e) 重点受托机构应具有足够的技术能力、人员队伍和设施、环境，满足托管服务的质量和安全管理要求。重点受托机构承担的托管服务场地应设置在中国境内。

f) 重点受托机构应具有完善的信息安全管理体系、业务连续性管理体系，并通过金融行业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。

5.2.1 受托机构的组织原则

受托机构的组织原则如下：

a) 受托机构应有专职团队负责托管维护服务的工作，如有参与托管维护服务的分包方，受托机构应具备对分包方的有效管理。

b) 受托机构应对托管维护服务中的不同角色有明确分工和职责定义。

c) 受托机构的岗位设置应按照“关键岗位不兼容”的原则，不兼容岗位之间禁止出现互相兼职的情况。

8.4.3 运行与维护

c) 受托机构同时为多家委托机构提供服务时，应对不同委托机构提供的服务资源相互进行逻辑隔离，仅委托机构具有对自身业务系统和数据的最高访问权限，保证不同委托机构的数据及系统运营安全，以满足监管要求。

8.5 业务连续性的保障和管理

a) 受托机构应按照银行业金融机构业务连续性管理相关监管要求，建立完善的业务连续性保障机制，包括业务连续性保障组织管理、业务中断时的决策机制、响应流程、处置策略、通知通告方式、业务恢复流程、审核与问责机制等。

8.6.4 重大服务风险的监控和报告

委托机构应对托管机构服务风险进行持续监控，发现以下事项时，应及时向监管机构报告：

d) 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。

e) 对风险监测和实地检查发现的问题，逾期仍未整改的。

自从上次业内知名的事故以来，规范化、标准化、监管细化将成为新的监管要求。

随着国民经济的发展，中小型银行需要更强的活力和竞争力，同时也面临更复杂的运行挑战和考验。相关托管服务机构准入机制，可能已经列入议程，从本规范已经可见端倪。

<u>尤其是重点受托机构</u>

3.6

重点受托机构 high-grade service provider

具有较高的集中度风险，其托管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，严重损害公众利益或造成银行业重大经济损失的机构。

注：重点受托机构提供的托管服务同时具备以下特点：

a) 承担集中存贮客户数据的业务交易系统托管服务；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生产中心、灾备中心机房及基础设施托管服务。

b) 重点受托机构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；或服务的国有、股份制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。

5.3.3 **重点受托机构的特定要求**

对于不同类型的托管服务，重点受托机构还应该满足：

a) 承担基础设施级托管服务的重点受托机构，其机房及基础设施应满足监管机构对数据中心、灾备中心的建设管理要求，应达到GB 50174—2008中规定的A级标准。

b) 承担重要信息系统灾备中心或灾难恢复服务的重点受托机构，宜具备国家或行业主管机构认可的灾难恢复资质。

c) 承担基础架构级托管服务的重点受托机构，要求具有完善的运行服务管理体系，并通过金融行业公认较为权威的运行服务管理资质认证。

d) 承担应用系统级托管服务的重点受托机构，要求具有完善的应用系统开发测试管理体系和运行服务管理体系，并通过金融行业公认较为权威的开发管理资质认证和运行服务管理资质认证。

e) 承担应用系统级托管服务的重点受托机构应建立同城灾备中心，其信息系统灾难恢复能力应达到GB/T 20988—2007中规定的5级（含）以上要求，并建立满足监管要求的异地灾备中心。

可能存在的新商机

6.2 服务需求的评估

c) 委托机构应对托管服务和受托机构可能引入的风险进行充分的分析和评估，根据风险评估的结果制定有效的风险管控策略和风险处置措施，以避免对委托机构业务产生不利影响。风险评估的结果应形成书面的风险评估报告，必要时可委托第三方专业机构对托管服务和受托机构进行专项风险评估工作。

7.5 服务方案的测试验证

c) 受托机构应按测试验证方案的内容向委托机构提供测试人员、准备测试环境、记录测试数据、提供测试报告，委托机构应提供必要的场地和人员协助，并对测试验证报告的结果进行验证。

8.2.2 监控和巡检管理

i) 应定期评估监控系统设计与执行的有效性，持续满足运维要求。

10.2 委托方审计

委托机构可以在符合法律、法规和监管要求的情况下，委托具备相应资质的外部审计机构对托管服务进行外部审计。委托方审计应满足以下要求：

10.3 独立第三方审计

在符合法律、法规和监管要求的情况下，委托机构或受托机构可以委托具备相应资质的外部审计机构对托管服务进行第三方审计。独立第三方审计应满足以下要求：

10.4 监管

监管机构可对托管服务进行非现场风险评估和现场检查，也可指定具备相应资质的外部审计机构对其进行审计。监管内容包括但不限于：

第三方检测、评估、审计相关单位如果做好充分的准备，将很可能收到相关红利。