ICS 35.240.40
A11

JR

中华人民共和国金融行业标准

JR/T 0140—2017

中小银行信息系统托管维护服务规范

Specification of information system hosting maintenance service for small and medium banks

2017-02-14 发布　　2017-02-14 实施

中国人民银行　　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由兴业银行股份有限公司提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准负责起草单位：兴业银行股份有限公司。

本标准参加起草单位：万国数据服务有限公司、上海翰纬信息科技有限公司。

本标准主要起草人：李坚宝、柯明通、李山河、詹志辉、徐光、姚昱全、左天祖、何政、陈宏峰、高勇、许志恒、江南春、唐宗、杨旭辉、欧阳捷、魏猛、姜克、李昀飞、马涛、刘世涛、张力强、饶祖广。

引　言

中小银行经过长期发展已经成为我国金融领域内重要的组成部分，如何在保证安全稳定的前提下，提高其资本使用效率，有效降低管理成本成为中小银行共同面临的难题。中小银行在信息系统的建设、使用和管理过程中普遍存在缺乏专业人员、管理体系不健全、系统建设不规范、系统功能不完备、系统更新不及时等问题，已经严重制约许多中小银行的发展。然而，中小银行独立建设功能全面的信息系统和管理规范的IT服务团队，存在建设成本高、周期长、效果不理想的难题。

银行信息系统承载了银行关键业务功能和敏感运营数据，信息系统的安全与稳定不但关系银行业金融机构的业务安全，同时也直接关系社会民生稳定和整个金融体系的安全。所以需要全面提升中小银行信息系统服务能力和水平，以确保银行信息系统的安全和稳定。

行业相关服务机构在建立专业共享资源、提供专业化服务方面已经积累了可资借鉴的服务产品和服务经验，可以向中小银行尤其是村镇银行提供包括基础设施托管服务、基础架构托管服务和应用系统托管服务在内的专业第三方托管维护服务。在可以预见的将来，随着中小银行的高速发展，信息系统托管维护服务必将在更大范围内普及和发展。

在信息系统托管维护服务快速发展的同时，如何安全、规范、有效的使用托管服务，做好服务过程的管理、服务质量的控制、降低信息安全风险成为各方面临的共同问题。为规范信息系统托管维护服务，持续改进服务水平，提高中小银行信息系统运行的安全性、稳定性，降低中小银行信息系统运行风险，满足中小银行的业务发展需求，特制定本标准。

中小银行信息系统托管维护服务规范

1 范围

本标准规定了中小银行信息系统托管维护服务生命周期各阶段的管理要求，包括托管前的准备、托管服务的建立、托管服务的持续保障、托管服务的变更和退出，以及托管服务的监督管理，规范了委托机构和受托机构双方应具备的资源准备、托管服务运行保障能力、托管流程以及管理机制，明确了信息系统托管服务的委托机构和受托机构双方的职责以及服务范围。

本标准适用于中小银行信息系统的托管维护服务。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范

GB 50174—2008 电子信息系统机房设计规范

3 术语和定义

下列术语和定义适用于本文件。

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。

3.2

信息系统 information system

由计算机系统、网络系统软硬件及其相关的设备、设施和应用软件等构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输和检索等处理的人机系统。

3.3

信息系统托管维护服务 information system hosting maintenance service

托管服务 hosting maintenance service

采用专业服务机构的基础设施环境，在此基础上将部分或全部信息系统服务（应用、数据、 IT 基础架构的优化、维护服务）委托给专业服务机构代为提供非驻场服务，以支持其自身的业务处理。

3.4

委托机构 client

托管服务的委托方和使用方。

注：本标准中委托机构限定于3.1中所述的中小银行。

3.5

受托机构 service provider

依法设立的信息系统托管维护服务的提供方。

注：受托机构包括村镇银行主发起行、银行业金融机构、专业服务提供商。

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。

3.7

生产中心 production center

委托机构对其业务、客户和管理等重要信息进行集中存储、处理和维护，具备专用场所，为业务运营及管理提供信息科技支撑服务的组织。

3.8

灾备中心 backup center for disaster recovery

委托机构为保障其业务连续性，在生产中心故障、停顿或瘫痪后，能够接替生产中心运行，具备专用场所，进行数据处理和支持重要业务持续运行的组织。

3.9

同城灾备中心 regional backup center for disaster recovery

与生产中心位于同一地理区域，一般距离数十公里，可防范火灾、建筑物破坏、电力或通信系统中断等事件的灾备中心。

3.10

异地灾备中心 non-regional backup center for disaster recovery

与生产中心处于不同地理区域，一般距离在数百公里以上，不会同时面临同类区域性灾难风险，如地震、台风和洪水等的灾备中心。

3.11

数据中心 data center

包括生产中心和灾备中心。

3.12

重要业务 critical business

面向客户、涉及账务处理、时效性要求较高的银行业务，其运营服务中断会对委托机构产生较大经济损失或声誉影响，或对公民、法人和其他组织的权益、社会秩序和公共利益、国家安全造成严重影响的业务。

3.13

重要信息系统 critical information system

支撑重要业务，其信息安全和服务质量关系公民、法人和组织的权益，或关系社会秩序、公共利益乃至国家安全的信息系统。

注：本标准中的信息系统指的面向客户、涉及账务处理且时效性要求较高的业务处理类、渠道类和涉及客户风险管理等业务的管理类信息系统，以及支撑系统运行的机房和网络等基础设施。

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。

4 综述

4.1 基本原则

信息系统托管维护服务的基本原则如下：

a) 权责明晰：委托机构和受托机构应清晰界定双方的职责分工、资产归属，明确交付内容和审查标准，并设立评审检查机制，明确违约责任和惩罚、赔偿原则。委托机构法定代表人是委托机构信息科技风险管理的第一责任人，委托机构不应将其信息科技管理责任外包。受托机构应建立配套的风险管理机制，配合完成委托机构的风险管理要求，以确保委托机构的利益和安全。

b) 信息安全：信息安全是开展信息系统托管维护服务的前提和基础，委托机构应明确托管服务的范围和安全等级要求，并针对不同安全等级明确信息安全策略。受托机构应针对委托机构的信息安全要求制定信息安全保障措施，并切实加强信息安全管理工作，确保委托机构的客户资料等敏感信息的安全。

c) 业务连续：信息系统托管维护服务应考虑意外事件可能导致的托管服务缺失对委托机构业务连续运营要求的影响，并设法将该影响减至最低。委托机构应明确本机构对托管服务业务连续性保障的目标要求，受托机构应建立恰当的应急措施和备用资源应对可能的风险。委托机构和受托机构都应建立完备的业务连续性计划，明确紧急状况下双方的分工和合作机制，并定期联合开展灾难恢复和业务连续性演练。

d) 资源共享：应统筹规划、适度集中、节约高效、合理利用信息科技资源。委托机构可采用发起行托管、同业共建或社会资源共享等方式获取信息系统维护服务资源，在选择共享方式时应综合考虑责任界定、信息安全和服务级别要求、区域集中风险和损失扩散等因素。

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：

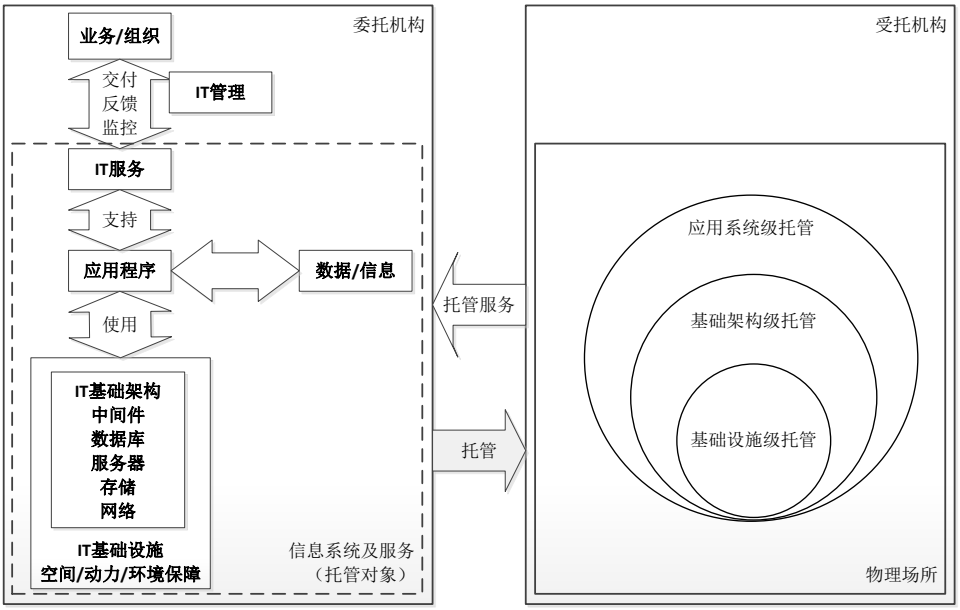

图1 托管维护服务范围和类型的示意图

4.3 信息系统托管维护服务生命周期

信息系统托管维护服务应包括以下几个阶段：

a) 托管前的准备：托管前委托方首先应对当前信息系统服务需求进行评估，明确必要的资源、服务内容和服务级别，明确双方对于当前信息系统所涉及的软件及数据知识产权使用情况，评估可能的资源获取方式和可能面临的风险、收益。根据确定的需求明确托管服务的服务项目和资源要求，审慎评估备选受托机构的资质、资格、资源保障能力、服务能力和服务经验，并与受托机构共同评估、规划、设计技术和服务方案。方案明确后将委托机构的基本情况、托管内容和范围、受托机构的基本情况、相关技术和服务方案等报送上级主管部门评审备案。

b) 托管服务的实现：委托机构与受托机构达成服务意向后签署正式的服务协议/合同，内容应明确服务内容、服务级别、双方权利、责任界定和发生合同偏离时进行处置的办法；受托机构按照签署的协议进行技术和服务方案的实施准备，并与委托机构共同完成受托系统和服务的建设

或迁移，在完成测试和试运行后签署书面验收报告。双方书面确认验收交付报告后进入正式服务期。

c) 托管服务的持续保障：在托管服务合同存续期间，受托机构应建立受托信息系统的服务规划和服务管理体系，确保达成约定的服务内容和服务级别，并定期提供服务达成情况的报告。委托机构在托管服务合同存续期间对受托机构进行定期评估，审查约定的服务目标和服务承诺的达成情况，审查服务管理过程的执行情况，并对受托机构定期进行审计。

d) 托管服务的变更和退出：委托机构在与受托机构合同谈判过程中应明确变更服务协议/合同的流程，以及委托机构或受托机构选择变更或终止服务协议/合同的条件，确保在中止服务协议/合同时收回或销毁受托机构保存的所有敏感信息和资料。当委托机构需求或受托机构服务保障能力发生重大变更时，双方根据事先约定的服务变更和退出流程妥善处理，调整服务协议/合同，处理遗留资产和信息，切实保障双方的利益和安全。

5 组织管理

5.1 委托机构的组织

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。

5.1.2 委托机构的管理职能

委托机构应建立专门的托管服务管理团队，完整的托管维护服务管理团队职能至少应包括：

a) 服务内容的管理职能，主要包括托管服务内容的选择、限定和过程管理等职能，具体包括：服务内容规划，服务目标、服务级别要求和服务范围的定义和审核，服务内容管理相关规范的制定、修订和审核，服务需求确认、服务资源建立、服务结果评估的过程控制等。

b) 服务机构的管理职能，主要包括受托机构的评价、选择和过程控制，具体包括：受托机构选择基准的设立、受托机构管理流程和制度的制定，受托机构的评价和选择，合同、协议的准备和审核签订，服务合同、协议的变更管理，合同违约的补偿和赔偿管理等。

c) 审计和评估的管理职能，主要包括对托管服务达成情况进行定期审计和评估，确保服务协议/合同的落实，具体包括：评估审计管理流程和制度的制定，服务质量标准的定义和考核，服务级别达成情况的评估，重大违规事件处置过程和结果的审计、评估，重大合同、协议变更过程和结果的审计、评估，关键风险控制措施执行情况的审计、评估等。

5.1.3 委托机构管理职能的实现

为实现5.1.2的职能，委托机构应按照自身业务特点、托管维护服务的范围、自身机构和人员构成等特点设定相应的组织架构和岗位，具体如下：

a) 委托机构应明确定义托管维护服务管理的主要负责人。

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。

c) 委托机构应设立专门的审计机构或岗位，定期检查服务过程或服务结果是否符合服务合同或协议的要求；对重大违规事件、重大合同和协议的变更应依据事先订立的审计标准，评估处理过程、结果的正确性及合理性。
d) 委托机构应设立专门的信息安全管理机构或岗位，评估托管维护过程中可能出现的信息安全风险，定期检查信息安全防护措施的有效性，协同处置托管维护过程中发生的信息安全事件。
e) 委托机构应保留服务过程、结果的完整记录，并定期对服务记录进行统计和回顾，建立服务评估和审计机制。

5.2 受托机构的组织

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。

5.2.2 受托机构的服务职能

一个完整的托管维护服务团队职能至少应包括：

a) 服务管理职能，主要包括服务策划和实现过程的内部管理，具体包括：服务体系规划设计、服务目标和服务范围定义、服务管理相关规范的制定和修订、服务级别达成情况的评估、服务协议/合同框架模板的制定、服务质量标准的定义和考核、内部审计、持续优化改善及机构管理职能（人力资源、财务管理、后勤保障等）的实现等。
b) 服务交付职能，主要包括服务需求确认、服务资源建立和服务结果反馈的过程管理，具体包括：服务方案的设计和确认、服务级别定义、服务协议/合同的拟定和签署、服务资源的建立和验证、服务请求的接收和反馈、客户投诉和建议的接收和反馈、服务报告的编制和递送、服务连续性与可用性管理、能力的规划和实现等。
c) 服务支持职能，主要包括服务过程具体资源和操作的管理，具体包括：服务请求的实现、事件的发现和处置、变更和配置的管理、应急响应和处置、问题的发现和解决、基础设施环境保障、信息安全等。

5.2.3 受托机构的服务职能的实现

为实现5.2.2的职能，受托机构应按照自身服务对象、服务范围、自身人员和能力构成等特点设定相应的组织架构和岗位，具体如下：

a) 受托机构应明确定义组织架构、岗位职能分工、人员技能要求、工作流程和操作规范，并依此建立人员上岗标准和培训、考核、晋升机制。
b) 受托机构应清晰记录 8.1 中要求的服务过程管理，定期对服务记录进行统计和回顾，建立服务评估和改进机制。
c) 受托机构应设立专门的客户服务机构或岗位，收集委托机构提出的需求、意见和建议并将响应结果及时反馈给委托机构。
d) 受托机构应设立专门的内部审计机构或岗位，检查服务过程、收集服务管理记录，并依据事先订立的审计标准评估检查结果，提出审计意见。

e) 受托机构应设立专门的信息安全管理机构或岗位，评估信息安全风险、管理信息安全策略、制定安全管理规程、管理信息安全事件、落实信息安全方案。
f) 受托机构应遵循“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，至少应保证执行和审计职能、开发和维护职能不可兼职。

5.3 受托机构的资质和能力要求

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。

5.3.2 组织和人员的能力要求

为保证托管维护服务的质量，受托机构的组织和人员的能力要求如下：

a) 受托机构应建立与托管服务相关的人员储备计划和机制，确保有足够的人员以满足和委托机构约定的已签和未来的托管服务需求。
b) 受托机构应建立与托管服务相关的培训体系或机制，并在制定培训计划时应识别培训要求，应提供及时有效的培训，并在培训结束后对培训效果进行回顾。
c) 受托机构应保证托管服务人员在学历教育基础上具备托管服务相关知识和技能，包括但不限于：基础设施操作能力、IT 设备和 IT 系统操作能力、系统工具管理能力。
d) 受托机构应配备与服务相适应的研发环境及研发队伍。
e) 重点受托机构的托管服务人员应具备从事相关服务的资格，特殊环境运行维护服务人员应具备在特殊环境下从事相关工作的资格。

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。

6 托管服务的准备

6.1 委托机构选择受托机构的基本原则

委托机构在选择受托机构时应充分考虑受托机构的服务能力、稳定性等风险，建立受托机构的准入标准，不因引入受托机构而增加整体剩余风险。

委托机构选择受托机构应遵循以下基本原则：

a) 委托机构应避免选择监管机构预警的高风险受托机构。

b) 受托机构应满足监管机构的准入要求。

c) 委托机构应审查、评估候选受托机构的财务稳定性和行业经验，对候选受托机构进行风险评估，考查其资源和能力是否足以承担相应的责任，防范引入高风险特性的受托机构。

d) 委托机构应对重点受托机构开展尽职调查，必要时可聘请第三方机构协助调查，在尽职调查时应关注：

——受托机构的技术和行业经验，包括但不限于：服务能力和支持技术、服务经验、服务人员技能、市场评价、监管评价等；

——受托机构的内部控制和管理能力，包括但不限于：内部控制机制和管理流程的完善程度、内部控制技术和工具、数据管理和访问控制方面的能力等；

——受托机构的持续经营状况，包括但不限于：财务状况、从业时间、市场地位及发展趋势等。

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。

b) 受托机构应对委托机构的需求进行深入研究，并以书面形式进行全面应答。应答书中应包括委托机构的具体需求描述、能否及如何保证满足委托机构的各项要求、以及达成这些要求的条件与假设，特别应如实说明服务中可能存在的风险。

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。

6.3 服务方案的设计

服务方案是受托机构向委托机构提供服务内容、服务范围、服务级别、服务方法以及对双方的限制限定等的总和。服务方案的设计应满足以下要求：

a) 委托机构和受托机构应根据托管需求共同建立完整的托管服务目录，明确托管服务的名称、内容、目标、关联关系、交付物，以便委托机构能根据自身的服务需求灵活地选择相关服务和定制服务方案。

b) 委托机构和受托机构应共同商定可检验、可量化的服务级别协议。服务级别协议应包括但不限于以下内容：

——托管服务的定性和定量绩效指标，以及每项指标的设置目标、标准；

——各项绩效指标的评估和考核机制，包括服务级别报告的提交、服务级别的定期评估制度、量化考核的方式等；

——服务级别考核结果与绩效之间的关系，包括不达标时应采取的措施。

c) 受托机构应依据托管服务目标和服务级别协议进行托管服务方案的设计，服务方案应涉及与托管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。

6.4 服务方案的评审和报备

服务方案的评审和报备要求如下：

a) 委托机构应对受托机构提交的服务方案和服务协议/合同进行客观、科学地评估和审核。

b) 受托机构提交的服务方案和服务协议/合同应经委托机构书面确认后方可开展托管服务。

c) 委托机构应对所有经审核的服务方案和相关审核记录进行备案，以下情况应向监管机构报备：

——数据中心整体服务托管；

——涉及客户资料、交易数据等敏感信息的服务托管；

——涉及集中存贮客户数据的业务交易系统的服务托管；

——其他监管机构认为重要的信息科技服务托管。

7 托管服务的建立

7.1 服务协议/合同的签署

委托机构应在开展托管服务前与受托机构签订服务协议/合同。服务协议/合同的签署应满足以下要求：

a) 服务协议/合同应包括但不限于：

——服务条款要求：包括服务范围、服务内容、服务价格、费用计算、服务期限、服务计划、服务方式、责任分配、交付物要求以及后续合作中的相关限定条件；

——交付要求：受托机构向委托机构提交详细的服务交付计划，包括服务交付时间、交付方式；

——合规与内控要求：对相关法律法规及银行业监管机构内部管理制度的合规要求、监管政策的通报贯彻机制、服务提供商的内控措施；

——服务连续性要求：受托机构的业务连续性管理目标应满足委托机构业务连续性目标要求；

——服务审核要求：委托机构对托管服务有监控和检查的权利，受托机构在服务期限内对委托机构的内、外部审计和监管机构开展延伸检查等方面有配合的责任；

——服务变更和终止要求：受托机构在过渡期间应履行的主要职责及合同变更或终止的过渡安排，包括信息、资料、软件、设备、设施等交接处置期间的相关服务安排；

——知识产权要求：明确托管服务过程中所产生、加工、交互的信息和知识产权的归属权，以及允许受托机构使用的内容及范围，对受托机构使用合法软、硬件产品的要求；
——服务级别要求：包括托管服务的关键要素、服务时效和可用性要求、数据的机密性和完整性要求、服务的变更控制要求、服务安全标准及业务连续性要求、技术支持要求等；
——服务报告要求：包括常规报告内容和提交频度要求、突发事件处置报告的提交流程、方式及时限要求等；
——服务的安全和保密性要求：明确受托机构在安全和保密方面的责任，以及针对安全及保密要求需采取的具体措施，并签署托管服务保密协议；
——服务转包与分包要求：在托管服务协议/合同中应要求受托机构不应将托管服务转包或变相转包，同时应明确服务分包的范围、责任、内容等方面的要求；
——违约条款：明确由于委托机构或托管机构责任导致的违约所需的赔偿、终止等行为发起、解决方式，必要时双方可约定购买商业保险增加赔付能力。

b) 委托机构与受托机构在签署托管服务协议/合同前，应重点考虑以下因素：
——托管服务协议/合同应包括允许委托机构监测和控制与托管服务相关的操作风险；
——托管服务协议/合同变更实施前后的平稳过渡（包括终止合同可能发生的情况）；
——托管服务协议/合同变更或终止所导致的业务连续性风险。

c) 托管服务级别协议和托管服务保密协议应作为托管服务协议/合同的附件与托管服务协议/合同主体具有同等的法律效力。

7.2 服务资源的准备

服务协议/合同签署后，受托机构应根据协议要求准备相应的服务资源。服务资源准备应满足以下要求：

a) 受托机构应按照托管服务的要求向委托机构提交服务资源准备方案，经委托机构审核后方可开展托管服务。

b) 受托机构应按照服务资源准备方案的要求向委托机构提供服务资源，包括但不限于场地、设备、设施、软件和工具、文档等，委托机构应依据银行业相关监管要求及托管服务协议/合同中的相关内容对服务资源进行必要的测试及验收。

7.3 服务人员的准备

服务协议/合同签署后，受托机构应根据协议要求准备相应的服务组织和人员。服务人员的准备应满足以下要求：

a) 受托机构应向委托机构提交满足托管服务要求的组织管理计划，包括组织架构、岗位职责及人员投入计划。

b) 受托机构应对其服务团队成员进行背景调查，确保其过往无犯罪或其他不良记录，且应与团队成员签订保密协议。

c) 委托机构应对受托机构的服务人员的资质、技能、经验、有无犯罪记录等背景信息进行审核。

d) 受托机构应及时根据托管服务的需要调整服务人员，包括撤换、补充、职责变更，以确保服务质量，关键岗位人员的变更和调整应及时通知委托机构。

7.4 服务管理的准备

服务协议/合同签署后，受托机构应根据协议要求进行管理体系、流程和标准的更新。服务管理的准备应满足以下要求：

a) 受托机构应向委托机构提交满足托管服务要求的服务管理计划，包括但不限于过程管理、操作管理、应用管理、信息系统安全管理、服务持续性管理。
b) 受托机构的管理体系应符合相关国际或国内标准并获得相关证明。

7.5 服务方案的测试验证

受托机构在服务资源、人员和管理方面准备就绪后应测试并验证服务方案的完备性。测试和验证应满足以下要求：

a) 为避免托管服务中存在技术和管理方面的缺陷，受托机构应依据服务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。
b) 受托机构应在测试验证前向委托机构提交测试验证方案，明确测试验证的方式、人员、环境、标准、文档等，委托机构应对测试验证方案进行评审。
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。

7.6 服务方案的交付

服务方案的交付应满足以下要求：

a) 受托机构向委托机构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，委托机构应对服务交付方案进行评审并与受托机构达成一致。
b) 委托机构应对受托机构提交的服务管理计划进行评审，并在服务交付过程中对受托机构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，应及时向受托机构反映，并要求受托机构采取必要的措施。
c) 服务交付完成后，受托机构应向委托机构提交服务交付报告，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，委托机构应组织相关人员对报告进行评审。

8 托管服务的持续保障

8.1 服务过程管理

8.1.1 服务请求和事件管理

受托机构应建立服务请求和事件管理机制，明确服务请求和事件管理流程，及时响应委托机构所托管的信息系统运行服务需求，提高事件处置效率，包括但不限于以下内容：

a) 应建立规范的服务请求和事件管理制度，就双方响应职责划分、响应级别、报警升级条件，通报和批准机制等内容达成共识，并形成书面文件。
b) 应提供服务级别保证，如服务范围、工作时间、响应时间等，明确响应支持的关键交付过程，并有措施保证交付过程的落地执行。
c) 应建立督促检查和升级机制，明确服务请求和事件管理的责任人，负责事件的记录、分级、分派、处理、监控、反馈和关闭整个流程。
d) 应建立便利的多样化的服务请求和事件接收渠道，保证接收渠道的便利和畅通。
e) 除了被动接收需求方的申报以外，应建立主动监控和预警机制，主动避免和减小对委托机构的业务影响。

f) 应根据事件的紧急程度和影响范围评估事件处理优先级，并在处理过程中设置技术升级和管理升级的流程，以确保合适的资源用于事件处理。
g) 当不能达到约定的服务级别或约定的活动时应及时通知委托机构，使其了解报告的事件或服务请求的进展。
h) 应专门定义重大事件及其响应、处理和通知机制，以便及时有效地进行应急响应，减少委托机构可能因此产生的损失，在重大事件发生时，应及时主动通报委托机构对其托管业务造成的影响和应对措施。
i) 应在给委托机构的服务报告中记录服务请求和事件的处理情况，并给出分析和改进建议。
j) 如需通过变更实施解决事件，应纳入变更管理审批后部署实施，变更管理流程应有委托方参与，经委托机构同意后方可实施变更。
k) 应定期回顾、分析事件处理记录，将重复发生的事件、重大事件、主动分析发现的隐患等纳入问题管理。
l) 应配合委托机构定期追踪、审计服务请求和事件管理的结果和记录，保证双方约定的管理机制得到切实的执行。

8.1.2 信息系统的配置和变更管理

受托机构应建立信息系统的配置和变更管理机制，明确配置和变更管理流程，明确双方工作界面，包括但不限于以下内容：

a) 受托机构应在托管服务建立过程中对受托管理对象建立资产和配置清单基线，并保证受托管理的资产和配置清单与实际环境保持一致。资产和配置清单的维护应保证完整、及时、准确、可追溯。
b) 受托机构应建立系统变更管理制度，对信息系统的硬件、软件、数据、机房环境等日常变更活动进行规范，明确双方工作界面和职责。应对变更的记录、分类、评估、批准进行管理。
c) 受托机构应明确系统变更中的角色，包括：申请人、评估人、审批人、实施人和配置管理员，审批过程应保留可审计记录，所有涉及到委托机构信息系统配置和更新的变更应通过委托机构的审批或获得委托机构的授权。
d) 受托机构应依据变更对象、影响范围、风险级别或紧急度的不同划分变更类别，并确定与变更类别相对应的审批路径，变更类别至少应包括：标准、一般、重大、紧急等。
e) 变更申请中应有明确的变更方案，内容包括但不限于：目标、时间、人员、操作步骤、实施方案、应急预案等，重大变更还应包括测试方案、回退方案和测试报告，审批人应组织评估变更的技术风险、业务风险，并制定相应的防控措施。
f) 重大变更应获得委托机构有权部门的同意，涉及生产系统和数据的重大变更应由委托机构有权部门审核确认。
g) 紧急变更应在事后补填变更方案和审批，影响或可能影响用户服务的紧急变更，应获得委托机构代表的口头授权，紧急变更成功后，应通过正常的验收测试和变更管理流程，采用恰当的修正以取代紧急变更。
h) 影响或可能影响用户服务的变更实施方案中应明确双方的工作范围和职责，对于以委托机构为主实施的变更实施方案，需要受托机构配合的应提前通知，并明确需要配合的内容和接口。
i) 变更实施前应先进行备份，以便必要时可以恢复原来的系统版本和数据文件。变更实施完成后配置管理员应及时更新基准配置信息。
j) 包括紧急变更在内的所有变更都应记入日志，由变更发起部门和变更实施部门共同审核确认。变更实施后应对变更的结果进行审查，审查内容应包括但不限于变更目标的达成情况、对生产环境的影响、配置库更新情况，审查结果应以报表形式定期发送至委托机构。

8.1.3 重大事件的处置

重大事件是指受托机构严重违反服务协议/合同约定或对委托机构造成重大损失的事件，包括但不限于因受托机构疏忽或不作为导致的服务等级降低、服务中断、人员财产损失和敏感信息泄露等。

重大事件的处置应满足以下要求：

a) 委托机构和受托机构应根据服务内容、服务范围和服务标准的界定，在服务协议/合同中事先约定事件等级标准和相应的处罚措施。
b) 受托机构应建立完备的风险评估和防范机制，对重大事件风险应进行事先的控制和规避。
c) 委托机构与受托机构应共同建立重大事件联合应急处置和响应机制。
d) 重大事件发生后受托机构应积极开展抢救、抢修和救治等应急处置措施，避免事故影响的扩大和蔓延。
e) 重大事件发生后受托机构应向委托机构主动提供事件情况的说明，包括但不限于：
   ——事件发生的原因；
   ——详细处置过程；
   ——造成的后果和损失；
   ——责任相关方的处罚；
   ——补救和赔偿方案；
   ——为避免类似情况再次发生采取的措施等。
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。

8.1.4 其他服务过程管理

除了8.1.1至8.1.3的管理要求外，受托机构还应开展以下服务过程管理：

a) 受托机构应建立有效的问题管理流程，及时响应信息系统运行问题，全面记录、分析和跟踪所有问题，直至问题解决；应对所有问题进行分类记录，并编制索引，提高同类问题的解决效率。
b) 受托机构应对问题的处理过程进行跟踪和管理，包括问题的识别、提交、分析、处理、升级、解决和关闭。
c) 受托机构应根据委托机构业务发展规划，配合委托机构制定符合其实际情况的能力规划，以适应由于外部环境变化产生的业务发展和交易量增长，能力规划应涵盖生产系统和备份系统。
d) 受托机构应对能力规划进行测量和跟踪，及时报告能力偏离，并根据委托机构要求对能力规划进行调整和修订。
e) 受托机构应建立文档和知识管理制度，并建立服务管理知识库，对服务过程中产生的事件描述、已知错误、解决方案、实施方案、应急措施和操作规程等文档进行有效管理。

8.2 操作管理

8.2.1 日常操作管理

受托机构在日常操作管理方面应符合以下要求：

a) 受托机构应设置独立的操作环境，设立门禁控制，并与开发、测试操作环境严格分离。
b) 受托机构应建立运行维护值班制度，并制定符合信息系统实际运维情况、流程清晰和内容明确的操作规程。
c) 受托机构应根据操作规程制定操作手册，操作手册应包括操作日程、操作对象、执行步骤和人员权限等基本要素，以及生产与开发环境中数据、软件的备份流程和要求。

d) 受托机构应严格按照操作手册执行运维操作，形成操作记录；关键操作过程要求双人临岗复核。
e) 受托机构应建立 7×24 小时现场监控和操作支持体系，并与二线技术团队、管理层和供应商等团队形成明确有效的升级协同机制。
f) 受托机构应按约定时限保存完整的操作记录，确保操作过程可追踪和可审计。

8.2.2 监控和巡检管理

受托机构在开展监控和巡检管理时应满足以下要求：

a) 应建立监控措施，选择合适的监控工具，对影响信息系统正常运行的关键对象，包括主机、存储、关键应用系统、数据库、网络、安全设备和通信线路等进行监控并及时预警，预警方式可包括声光、电话、短信和邮件等。
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。
c) 应建立辅助的人工巡检机制，规定巡检内容、频度和人员等，并采取有效的技术和管理措施确保巡检活动按承诺的质量和频率得到切实执行。
d) 巡检内容应涵盖物理设施、软硬件运行环境和应用执行状况等事项，巡检结果应及时记录，如遇异常应及时处理，按规定要求进行报告。
e) 应明确监控对象的主要监控指标和覆盖范围，对于自动化监控的指标应明确缺省预警阈值，所有监控指标应定期进行评估和更新。
f) 服务方案应对监控报警的场景和应对处置流程有明确清晰的定义。
g) 应定期分析监控日志，评估信息系统运行状态，跟踪处理日志分析中发现的异常事件，并形成评估报告。
h) 应建立有效的信息系统运行日志管理流程，对信息系统日志实行分级管理，对重要日志进行定期备份，确保安全事件发生时有据可查，并满足审计的需要。
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。

8.2.3 数据管理

受托机构在开展数据管理时应满足以下要求：

a) 数据管理包括电子数据、纸质数据以及存放相关数据信息介质的管理。
b) 受托机构应与委托机构协商确定数据管理策略，包括：数据类别、数据安全等级和保护措施，数据收集、使用、修改、备份和检查的管理原则等，数据管理策略应满足监管和法规要求。
c) 受托机构应根据确定的数据管理策略建立数据管理规程，明确数据管理的具体办法和措施，并对介质的递送、存放、使用、维护和销毁等方面做出规定。
d) 受托机构应制定数据保管、备份及验证策略，明确备份范围、备份方式、备份频度、责任人、存放地点和有效性验证方法。并按照所制定管理策略的要求，对数据的完整性、可用性进行定期验证。
e) 受托机构应根据约定期限保留所有委托机构数据的维护记录，包括数据来源、数据分类、分级，以及收集、使用、修改、备份、检查和销毁过程的记录。
f) 受托机构应根据服务对象和服务需求，明确自身生产环境正常运行所需的重要业务数据、系统数据的备份策略和备份方法等，以响应和支持用户服务的恢复。

8.3 应用管理

8.3.1 需求管理

受托机构在开展软件需求管理时应满足如下要求：

a) 应与委托机构就需求管理进行约定，将开发需求纳入项目管理体系，确保业务需求得到及时响应。
b) 应规范软件项目需求评审活动，组织项目干系人共同识别需求和需求风险，与委托机构共同确认需求范围。评审专家应由业务专家和技术专家组成。
c) 应建立用户需求管理制度及工作流程，包括但不限于需求的提出、分析、评审、变更、跟踪、用户确认等环节。
d) 应建立需求跟踪机制，并定期向委托机构报告实施进度，及时发现遗漏、错误的理解和不一致性，以便及时加以纠正。
e) 应建立需求变更控制流程，当系统需求发生变更时，应遵循变更流程实施变更，并及时更新相关文档。

8.3.2 开发管理

受托机构在开展软件开发管理时应满足如下要求：

a) 应制定科学的开发制度，确保软件设计满足安全要求、监管标准和编码规范，保证代码的一致性、兼容性和可维护性。
b) 应根据服务约定与委托机构确定开发计划，软件开发过程各阶段的任务、要求和交付文件等应有明确要求，实现软件开发过程的标准化，并及时通报开发进度。
c) 应当充分考虑系统稳定性、安全性、可靠性和可扩展性，明确系统体系结构、组件模块划分、模块控制的流程、接口和数据结构等内容，确保覆盖系统需求范围，支持需求与设计双向跟踪。
d) 涉及历史数据迁移的开发需求，应制定切实可行的数据迁移方案，并验证数据有效性，确保迁移后数据的完整性、安全性和可用性。
e) 应建立开发单元自测机制，测试应覆盖系统功能的各分支流程。
f) 开发过程中设计、计划等文件的补充和修订，应通过周密的控制以保持文件与程序产品的一致性，保持各种文件之间的一致性和文件的安全性。
g) 应将生产系统与开发系统、测试系统的管理职能进行分离， 禁止开发人员进入生产系统，确保生产环境及系统的可靠性、完整性和可维护性。

8.3.3 测试管理

受托机构在开展软件测试管理时应满足如下要求：

a) 应对系统上线运行前的测试工作进行规范管理，由需求提出方组织测试并对测试过程进行审查。
b) 应通过主机分离、物理隔离和操作环境分离等方法把测试环境与生产环境严格隔离。
c) 应对测试结果和测试方给出的测试报告进行分析评估，确定是否可以投产。

8.3.4 投产管理

受托机构在开展软件投产管理时应满足如下要求：

a) 应当建立投产评审、审批和部署等制度，规范投产管理流程，充分识别并控制投产及变更可能造成的操作风险、法律风险和声誉风险。
b) 应与委托机构共同制定系统回退和应急处置计划和流程，必要时应实施演练。
c) 应根据委托机构的上线要求安排投产，并由委托机构在生产环境上及时进行验证。
d) 应在信息系统投产后一定时期内持续跟踪运行情况，确保系统安全稳定运行。

8.3.5 版本管理

受托机构在开展版本管理时应满足如下要求：

a) 应与委托机构在服务方案中明确需要纳入版本管理的范围，对约定范围内的源代码和文档版本进行分类管理。
b) 应建立统一的版本管理制度，并与委托机构预先确定受托机构统一版本还是委托机构独立版本。
c) 应建立版本的访问控制和备份管理，以防止意外修改、泄露和丢失，保障版本的安全性、一致性和可恢复性。
d) 应与受托机构就版本升级事项进行约定，把版本升级纳入版本管理的控制之下，提供严格定义的升级方法，谨慎地控制版本的升级。

8.4 信息系统安全的保障和管理

8.4.1 风险管理

开展信息科技风险管理时应满足如下要求：

a) 受托机构应组织评估本机构面临风险状况，找出可能影响委托机构服务结果和服务承诺的风险要素，制定受托机构的风险管理策略。
b) 受托机构应定期开展风险评估工作，向委托机构提供本机构风险评估的结论，并依此决定采取风险防范的措施和方法，对风险进行分级管理。
c) 受托机构应建立健全各项管理与内控制度，设立专门风险管理岗位，监督和检查各项规范、制度、标准和流程的执行情况以及风险管理状况，持续监督风险管理状况，及时预警，将风险控制在可接受水平。
d) 受托机构应建立信息安全事件管理机制，定期向委托机构提供信息安全事件统计和跟踪改进的报告，重大信息安全事件应随时报告。
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。

8.4.2 系统开发和测试

受托机构在开展系统开发和测试时应满足如下要求：

a) 受托机构应制定有效办法确保所管理的信息系统源码的完整性和保密性，可采取的措施包括但不限于：
   ——建立源码管理机制和管理平台，保证系统源码完整并得到及时的更新；
   ——建立源码备份管理机制，源码应定期备份并离线异地保管；
   ——源码的保管和备份应执行加密和授权管理机制，避免源码泄露；
   ——源码的分发、变更、备份和上线过程应保留完整记录，以供审查和审计。
b) 受托机构应建立严格测试环境和测试数据管理机制：
   ——测试系统中使用的敏感测试数据应进行脱敏处理；
   ——测试完成后应对测试环境进行清理，包括测试中使用的数据、资料等；
   ——测试完成后应对测试过程使用的接口，特殊权限等进行清理和关闭；
   ——测试中发现的问题应加以保管，避免被无关人员获取利用。

8.4.3 运行与维护

受托机构应确保受托管理对象的可靠性、完整性和可维护性，在进行运行与维护时应满足如下要求：

a) 除得到委托机构授权批准外，禁止受托机构应用程序开发和维护人员进入生产系统。

b) 受托机构应确保设立物理安全保护区域，包括计算机中心或数据中心、存储机密信息或放置网络设备等重要信息科技设备的区域，明确相应的职责，采取必要的预防、检测和恢复控制措施。应严格控制第三方人员进入安全区域，如确需进入应得到适当的批准，其活动也应受到监控。

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。

d) 受托机构应根据信息安全级别，将网络划分为不同的逻辑安全域（以下简称为域）。应该对下列安全因素进行评估，并根据安全级别定义和评估结果实施有效的安全控制，如对每个域和整个网络进行物理或逻辑分区、实现网络内容过滤、逻辑访问控制、传输加密、网络监控和记录活动日志等。

e) 受托机构应确保所有计算机操作系统和系统软件的安全：

——制定不同类型操作系统的安全策略，明确定义不同用户的访问权限；

——制定账户权限的审批、验证和监控流程，确保最高权限用户的操作日志被记录和监察；

——定期检查可用的安全补丁，并报告补丁管理状态。

f) 受托机构应确保所有信息系统的安全：

——明确定义维护人员在信息系统安全中的角色和职责；

——采取有效的身份验证方法，对关键或敏感岗位进行双重控制；

——在关键的接合点进行输入验证或输出核对；

——应根据监管机构的要求，做好应用系统安全测评和安全性测试，避免委托机构客户信息等重要资产外泄；

——明确定义例外情况的处置机制；

——以书面或电子格式保存审计痕迹。

g) 受托机构应制定相关策略和流程，管理所有生产系统的活动日志，以支持有效的审核、安全取证分析和预防欺诈。应保证交易日志和系统日志中包含足够的内容，以便完成有效的内部控制、解决系统故障和满足审计需要。

h) 受托机构应针对长期或临时聘用的技术人员和承包商，制定审查程序，包括身份验证和背景调查。

i) 受托机构维护人员离职或岗位变动时，应在系统中及时检查、更新或注销其身份，修改该人员所管理的服务器、数据库系统的静态口令，并对重要岗位人员制定脱密期。

j) 受托机构在选择数据中心的地理位置时，应充分考虑环境威胁，并采取有效的物理控制措施。

k) 受托机构应建立全面的制度和措施，严格控制对关键设备和数据的接触与移动，具体措施包括但不限于：安防监控、人员登记、人员识别、权限控制和物理隔离等措施。

l) 受托机构应建立有效管理用户认证和访问控制的流程。建立与信息访问级别相匹配的认证机制，并且确保其在信息系统内的活动只限于相关业务能合法开展所要求的最低限度。

m) 受托机构应建立资产安全和数据安全管理制度，对托管设备、系统和数据进行分类和标识，对设备和存储介质应进行全生命周期的有效管理，防止设备和介质上的信息泄露。

n) 受托机构应严格控制远程访问管理的设备和渠道，特别是开放公共端的远程访问应包括人工身份确认在内的双因素身份认证。

o) 应建立病毒监测和防范机制，所有接入工作网络的台式机和移动终端应安装适当的杀病毒软件，并采用集中式的防病毒管理工具。

p) 重要信息系统维护操作应建立集中权限控制和操作审计平台，保证所有操作过程可追踪可审计。

q) 应建立移动介质管理机制，严格限制U盘、移动硬盘等移动介质的使用，通过技术手段防范受托方内部人员拷贝敏感数据和用户信息，并防止经由使用移动存储介质感染计算机病毒或木马的途径，杜绝生产环境与非生产环境各种间接的、非必要的和不受控的通讯访问。

8.4.4 客户信息安全

委托机构应在托管维护服务关系成立之前评估托管系统中客户信息风险，并明确防范措施。受托机构应制定相关制度和流程，严格管理客户信息的采集、处理、存贮、传输、分发、备份、恢复、清理和销毁。相关制度和流程包括：

a) 受托机构应采取加密技术，防范涉密信息在传输、处理和存贮过程中出现泄露或被篡改的风险，并建立密码设备管理制度。

b) 受托机构应建立明确的客户信息查询流程，根据人员岗位职责，严格控制敏感客户信息查询权限及客户信息打印和导出功能。

c) 受托机构应建立客户信息更新流程，确保客户信息更新操作得到委托机构授权，更新操作有可靠记录以备审计跟踪，更新后的信息得到审核校验。

d) 受托机构应加强客户信息提取管理，制定详细的操作流程，确保客户信息提取得到委托机构授权，对客户信息的提取操作进行监控与记录。受托机构与委托机构应建立专门的客户信息交接机制。

e) 受托机构对客户信息更新及敏感客户信息查询、提取操作应实行双人操作。

f) 受托机构应对包含客户信息的备份数据采取防护措施，应在委托机构监督下，对过期数据及报废存储介质单独进行销毁，受托机构应确保销毁过程不可逆。

8.5 业务连续性的保障和管理

受托机构在进行业务连续性的保障和管理时应满足如下要求：

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。

b) 受托机构应充分考虑托管服务对委托机构业务连续性管理的影响，在托管服务期间有计划、有针对性的完善业务连续性管理计划，包括但不限于：

——识别重要业务所涉及的服务资源；

——制定业务中断时的应急资源保障计划；

——制定业务中断时的人力资源保障措施；

——对托管服务过程中的业务连续性管理能力和水平进行定期监控和评价；

——定期组织业务连续性计划演练，并对业务连续性计划进行修订和完善。

c) 受托机构应配合委托机构建立业务连续性管理风险控制、缓释或转移措施，包括但不限于以下内容：

——采取相应的手段预测和提早发现可能导致业务中断的潜在因素；

——制定关键业务中断时的手工业务恢复机制及数据追补措施；

——制定业务中断的应急处理流程。

d) 委托机构和受托机构应建立业务连续性的联动机制，明确紧急事件处置的联络机制和授权机制，共同制定有效的应急响应和灾难恢复计划，并定期进行联合演练。

8.6 服务的持续监督和改善

8.6.1 服务监督机制

受托机构的服务监督机制应满足以下要求：

a) 受托机构应建立服务监督机制，对服务过程进行持续监控，明确阶段性服务目标及任务，并跟踪任务的执行情况，及时发现和纠正服务过程中存在的各类异常情况，定期向委托机构提供相关服务报告和报表。
b) 受托机构应当建立明确的服务目录，服务级别协议以及服务级别监控评价机制，确保服务监控基础数据和评价结果的真实性和完整性，数据至少需保存到服务结束后一年。
c) 受托机构应建立服务满意度调查机制，对服务过程进行客户满意度调查，对满意度低的服务进行评审回顾和分析，并限期改进。
d) 受托机构应建立服务投诉和申诉渠道，及时响应和处理委托机构对服务的投诉和建议，响应接口不能处理的投诉时，应具备相应的升级渠道，以便受托机构高层管理人员介入投诉处理。

8.6.2 服务的监控和管理

受托机构应当根据委托机构的服务需求、合同和服务级别协议等建立明确的服务质量监控指标，并进行相应的监控。指标包括但不限于：

a) 稳定性指标：
——信息系统、设备及基础设施的可用率；
——应用系统交易成功率；
——投产变更成功率；
——程序的缺陷数；
——故障次数、故障解决率、故障的响应时间。
b) 安全性指标：
——假冒网站查封率；
——外部攻击变化率；
——安全事件数量。
c) 服务性指标：
——服务的次数、客户满意度；
——服务人员工作饱和率、服务人员的考核合格率；
——各阶段业务需求的及时完成率、需求变更率。
d) 规模性指标：
——主要电子渠道交易变化率；
——主要电子渠道活跃用户、账户变化率。

8.6.3 服务优化改善

受托机构在进行服务优化改善时应满足以下要求：

a) 受托机构应借鉴和采纳业内成熟的服务管理框架和最佳实践经验，采用 PDCA 方式定期回顾、审视和评估承担的托管服务状况，实现持续改进。
b) 受托机构应充分重视委托机构在服务过程中提出的投诉、意见和建议，建立相应的跟进机制调查原因，制定措施，实施改进并反馈到委托机构。

c) 受托机构应充分重视托管服务过程中发生的高优先级告警和事件，组织相关部门调查事件处理的全过程，明确告警和事件发生的根本原因，寻找可能的改进和弥补之处，并提交正式服务报告给委托机构。
d) 受托机构应建立严密完整的质量控制体系，通过部门自查、部门之间交叉检查、机构内审和外部专业机构审计结合的方法，对照成熟的服务体系规范、对委托机构的服务级别承诺和业内高水平的服务标准寻找优化改善的地方，并有明确的流程和规定，进行跟踪和评估。
e) 受托机构应定期向委托机构提交服务报告，并与委托机构定期或不定期举行会议讨论服务报告，获取服务反馈和建议，报告内容包括但不限于服务请求响应和事件的统计，相关服务指标的统计，服务状况的综述和服务改进建议等。
f) 受托机构的优化改善方案应包括技术优化和管理优化等方面，优化改善方案宜包含目标、内容、步骤、人员、预算、进度和衡量指标，涉及变更的还需有风险预案和回退方案；对优化改进方案进行必要的评审，按优化改善方案实施并安排观察期，在优化改善完成后进行必要的回顾总结，并对遗留问题制定改进措施并跟踪。

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：

a) 违反国家法律、法规和监管政策，情节严重的。
b) 窃取、泄露银行业金融机构敏感信息，情节严重的。
c) 因管理过失，多次发生重要信息系统服务中断或数据损毁、丢失和泄露事件的。
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。
f) 存在其他违法违规行为，或发生其他重大信息科技风险事件的。

9 托管服务的变更和退出

9.1 托管服务变更管理

9.1.1 服务变更的发起

托管服务的服务内容、范围和标准要求等可能由于委托机构服务需求的变化或受托机构服务资源、服务能力的变化而进行调整。服务变更的发起应满足以下要求：

a) 委托机构发起服务变更请求，受托机构应及时响应，并在规定的时间内进行反馈。反馈的内容包括：
——双方就服务变更确认后，受托机构应细化变更服务方案、实施计划和恢复方案等；
——受托机构应提出服务内容相匹配的服务内容说明及服务级别承诺；
——变更的服务内容及服务级别应以合同方式体现。
b) 受托机构发起服务变更，应提出变更的方案，并与委托机构协商确定变更方案，变更方案应：
——明确变更带来的风险，提出风险防范计划，制定风险管控与抵御措施；
——提出明确的时间计划，并与委托机构充分协商，审核确认，避开银行业务运行敏感时间窗口；
——如由于受托机构的重大组织变化、资源变更、战略转型等需要进行重大变更，应事先向委托机构发起申请，为双方协商和托管服务的平稳过渡预留足够时间。

9.1.2 服务变更的风险控制

受托机构应配合委托机构对变更服务方案进行风险评估，并根据风险评估结果，采取必要措施控制变更风险，评估内容至少应包括：

a) 基础架构运行风险评估。
b) 技术性风险评估。
c) 服务经验风险评估。
d) 服务人员风险评估。
e) 合规性风险评估。
f) 操作性风险评估。

9.1.3 突发性变更及终止服务

受托机构如因自身机构重组、突发性破产和重大人员流失等原因导致突发性的服务变更或服务终止，双方应：

a) 严格按照合同规定，履行双方责任和义务。
b) 委托机构应按照事先准备的服务中断应急预案处置。
c) 受托机构应协助委托机构，在服务变更或终止过程中，保证系统的有效运行。
d) 受托机构应协助委托机构顺利完成服务交接。

9.2 托管服务退出管理

9.2.1 服务退出的发起

托管服务由于情况变化、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：

a) 在服务协议/合同到期前，委托机构应以书面方式明确退出服务协议/合同，受托机构应及时响应，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。
b) 需提前结束服务的，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，并为双方协商和托管服务的平稳过渡预留足够时间。

9.2.2 服务退出的风险控制

服务退出时委托机构应充分考虑服务退出带来的影响，采取必要措施控制退出风险。服务退出的风险控制应满足以下要求：

a) 委托机构和受托机构在签署服务协议/合同时就应明确可能的退出机制和退出方案。服务协议/合同中至少应约定：
   ——正常服务到期时间；
   ——预留的服务交接周期；
   ——服务交接的机制；
   ——服务数据保密的延续周期；
   ——服务质量不能满足合同要求的情况下服务资源的优先权；
   ——如果涉及到知识产权，还应制订交接及转让细则。
b) 双方还应在服务协议/合同或服务协议/合同附件中包含服务退出后的资源的处置方案，包括但不限于：
   ——设备及信息系统的搬迁方案；
   ——关键的数据资源迁移或销毁方案；
   ——服务期内租用的 IT 设备的交接及数据清除方案；

——服务期内产生的文档、数据介质、电子记录等的回收、交接与销毁方案；
——通讯网络的转移或解除租用方案；
——涉及到数据资产的保密协议。

c) 委托机构和受托机构应采取有效措施规避托管服务非计划退出的风险，包括但不限于：
——委托机构应充分评估托管服务中断可能产生的影响，对于涉及重要业务的托管服务，应预先配置备选或可替代资源，保证最低限度的服务能力；
——委托机构应与受托机构共同建立应急响应计划和措施，并定期组织应急演练；
——受托机构应急响应机制和预案发生重大变化时应书面通知委托机构；
——受托机构发生可能造成托管服务能力不足或终止的潜在风险时应及时通报委托机构。

d) 由于不可抗力等因素导致计划外退出的，双方应采取措施积极补救，在优先考虑减低风险和损失的前提下根据双方责任大小确定赔偿或补偿办法。

10 托管服务的监督管理

10.1 内部审计

10.1.1 内审制度的建立和执行

受托机构应建立内部审计制度，内部审计部门应根据服务的性质、规模和复杂程度，对相关服务内容及其管理的适当性和有效性进行审计。参与审计的信息科技审计人员应具备相应的专业能力并独立于服务的日常活动。内部审计包括全面审计和专项审计，其中，专项审计，是指对托管服务安全事故进行的调查、分析和评估，或审计部门根据风险评估结果对认为必要的特殊事项进行的审计，审计步骤应包括：

a) 制定、实施和调整审计计划，检查和评估服务过程的充分性和有效性。
b) 按照内审制度规定完成审计工作，在此基础上提出整改意见，并检查整改意见是否得到落实。

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。

10.2 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：

a) 委托机构应与外部审计机构进行充分沟通，确定审计的具体范围。
b) 委托机构应确保外部审计机构能够对托管服务涉及的硬件、软件、文档和数据（国家法律、法规及监管机构规章、规范性文件规定的重要商业、技术保密信息除外）进行检查，以发现托管服务存在的风险。
c) 受托机构应予以配合，并提供相关资料、数据和报表，不应故意隐瞒事实或阻挠审计检查。
d) 受托机构应根据审计报告提出整改计划，并在约定时间内实施整改。

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：

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。
b) 委托机构或受托机构在委托外部审计机构进行外部审计时，应与其签订保密协议，并督促其严格遵守法律法规，保守本机构的商业秘密和信息科技风险信息，防止其擅自对受托机构提供的任何文件进行修改、复制或带离现场。

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：

a) 监管机构可根据对托管服务非现场风险评估和现场检查的结果，对其发出监管提示通知，委托机构及受托机构应根据监管提示制定整改计划，并在规定时间内实施整改。
b) 外部审计机构根据监管机构的授权对委托机构及受托机构进行审计时，应出示委托授权书，并依照委托授权书上规定的范围进行审计。
c) 外部审计机构根据授权出具的审计报告，经其授权监管机构审阅批准后具有与授权监管机构出具的检查报告同等的效力，委托机构及受托机构应根据该审计报告提出整改计划，并在规定时间内实施整改。

参 考 文 献

[1] GB/T 24405.1—2009 信息技术 服务管理 第1部分：规范

[2] GB/T 28827.1—2012 信息技术服务 运行维护 第1部分：通用要求

[3] JR/T 0011—2004 银行集中式数据中心规范

[4] JR/T 0044—2008 银行业信息系统灾难恢复管理规范

[5] 中国人民银行.中国人民银行计算机系统信息安全管理规定（银发〔2010〕276号）.2010年9月27日.

[6] 中国银行业监督管理委员会.商业银行信息科技风险管理指引（银监发〔2009〕19号文印发）.2009年6月1日.

[7] 中国银行业监督管理委员会.商业银行数据中心监管指引(银监发〔2010〕114号文印发).2010年4月20日.

[8] 中国银行业监督管理委员会.商业银行业务连续性监管指引（银监发〔2011〕104号文印发）.2011年12月28日.

[9] 中国银行业监督管理委员会.银行业金融机构信息科技外包风险管理指引（银监发〔2013〕5号文印发）.2013年2月16日.