团 体 标 准

T/CCUA/ 004-2018

金融信息技术服务外包风险管理能力
成熟度评估规范

Risk management norms for outsourcing of financial information technology services
(征求意见稿)

目 次

前言	IV
引言	V
1 范围	6
2 规范性引用文件	6
3 术语和定义	6
第一部分：总体要求	9
4 金融信息科技服务外包风险管理能力成熟度评价体系	9
5 发包方能力成熟度规范	10
6 承包方能力成熟度规范	14
第二部分：发包方成熟度分级准则	19
7 发包方成熟度级别概述	19
8 第 I 级	19
9 第 II 级	21
10 第 III 级	23
11 第 IV 级	25
12 第 V 级	28
第三部分：承包方成熟度分级准则	32
13 承包方成熟度级别概述	32
14 第 I 级	33
15 第 II 级	35
16 第 III 级	37
17 第 IV 级	41
18 第 V 级	45
第四部分：评估的基本原则和流程	50

19 评估基本原则	50
20 评估流程	51
21 定级的有效期	52
参考文献	53

前 言

本标准按照GB/T 1.1—2009有关规则起草。

本标准由中国计算机用户协会信息科技审计分会提出并归口。

本标准起草单位：中国计算机用户协会信息科技审计分会、华夏银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、交通银行股份有限公司、深圳前海微众银行股份有限公司、中国银河证券股份有限公司、农信银资金清算中心、国家开发银行、招商银行股份有限公司、上海浦东发展银行股份有限公司、恒丰银行股份有限公司、福建省农村信用社联合社、广州银行股份有限公司、山东重工集团财务有限公司、山东省城市商业银行合作联盟有限公司、中治研（北京）国际信息技术研究院、北京信息科技大学、南京审计大学、建投数据科技股份有限公司、北京志翔科技股份有限公司、北京中润长弘管理咨询有限公司、华为技术有限公司、北京先进数通信息技术股份公司。

本标准主要起草人：李印波、苟海儒、韩建国、姜健、周正明、洪振龙、蔡睿、刘园、薛艳春、窦春坦、颜涵、林创、何乃煜、高立君、李海龙、李治平、肖君君、余小兵、崔国玺、赵新平、刘丹、李长征、俞文平、高巍、侯惠文、罗慧萍、黄泽敏。

引 言

近半个世纪以来，我国金融科技从无到有，经历了电子化、信息化、网络化和数字化等阶段，现在进入了全球先进行列，为实现普惠金融和金融现代化奠定了坚实基础。与此相伴，金融科技外包服务产业也逐步形成，并发展壮大，对促进我国金融现代化建设发挥了重要作用。随着金融对信息科技依赖度的不断提高，信息科技外包服务能力和水平对现代金融服务水平和质量的影响越来越大。同时，信息科技服务外包行为不规范所导致的金融机构服务风险日趋严峻，甚至形成行业风险，已引起金融机构和监管部门的高度重视。

本标准的建立，有利于行业组织开展行业自律，对推进落实金融风险管控和监管目标提供行业性和系统性支撑，对促进金融科技服务外包行业健康合规发展和良好生态形成具有建设性作用。有利于规范和有效控制金融机构信息科技服务外包风险，规范承包机构行为，并为第三方评估机构开展外包风险评估提供了标准依照。

金融信息科技服务外包风险管理能力 成熟度评估规范

1 范围

本标准规定了金融业信息科技服务外包风险管理能力成熟度评价体系，规定了发包方和承包方的总体要求；并对发包方、承包方的外包风险管理能力成熟度进行了分级和定义；规定了对发包方和承包方进行风险管理能力成熟度评估的基本原则和流程。

本标准适用于金融行业信息科技服务外包活动中的发包方、承包方和第三方评估机构。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅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 22080-2016 信息技术 安全技术 信息安全管理体系 要求

GB/T 24405.1-2009 信息技术 服务管理 第1部分：规范

JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引

3 术语和定义

3.1

信息科技服务 information technology service

组织为了实现组织目标所开展的一系列获取所需信息科技能力的活动。常见的服务内容包含有信息科技咨询服务、设计与开发服务、测试与评估服务、信息系统集成服务、数据处理与云服务、运营与维护服务、人力资源服务等。

3.2

信息技术服务外包 information technology service outsourcing

组织将部分或全部信息技术服务委托给其他组织完成，以提高效率，降低成本，优化产业链，提升组织的核心竞争力的管理模式或商业行为。

3.3

信息技术服务外包风险 information technology service outsourcing risk

信息技术服务外包过程中，诸多不确定性对组织目标产生的影响。

3.4

外包风险管理 outsourcing risk management

对信息技术服务外包风险进行有效控制的组织措施和机制。

3.5

金融监管机构 financial regulator

对金融风险实施行业监管的国家有关部门。

3.6

发包方 outsourcing contractee

信息技术服务外包的需方。

3.7

承包方 outsourcing contractor

信息技术服务的提供方。

3.8

第三方评估机构 Third - party assessment entity

依据相关规定，对信息技术外包服务风险管理能力进行综合评价的组织。

3.9

服务目录 service catalogue

服务提供方提供的标准服务的列表。

3.10

服务级别 service level

描述服务达到的水平。一般通过服务质量、服务效率、服务应用性以及信息安全等方面进行衡量。

3.11

服务级别协议 (SLA) service level agreement (SLA)

服务提供方与发包方之间签署的、描述服务和约定服务级别的协议。

[GB/T 24405.1—2009, 定义2.13]

3.12

发包方能力成熟度 maturity level of outsourcing contractee ability

体现发包方对信息科技服务外包的有效管理和控制程度的一种综合指标。

3.13

承包方能力成熟度 maturity level of service provider ability

体现承包方的信息科技服务承包能力的一种综合指标。

3.14

关键人员 key person

对信息科技服务外包的进度和质量有重大影响的承包方服务实施人员。

3.15

人员流失率 talent loss rate

在所统计的年度，从信息科技服务团队离开的人员占服务团队总人数的比例。

第一部分：总体要求

4 金融信息技术服务外包风险管理能力成熟度评价体系

4.1 总体目标

金融信息技术服务外包风险管理能力成熟度评价体系的目的是促进金融行业服务外包过程中各行为主体和要素相互积极作用，形成良好生态场景。相关组织应在信息技术服务外包活动中建立、实施、运行、监视、评审、保持和持续改进信息技术服务外包风险管理能力。

4.2 成熟度模型

信息技术服务外包风险管理能力成熟度模型是由发包方对自身的服务外包风险管理和承包方对自身的两个PDCA循环构成的过程模型，组织通过建立(Plan)、实施(Do)、监控评估(Check)和持续改进(Act)来完成金融信息技术服务外包风险管理能力的建立和持续改进。

4.2.1 发包方能力成熟度模型

发包方应从战略管理、组织与制度管理、流程管理、质量管理、风险管理、信息安全管理、合规管理和工具管理等方面建立服务外包风险管理能力模型规范。按照能力模型规范的要求，结合组织的具体情况进行实施，同时对建立服务外包风险管理体系的效果进行监控评估，并根据评估结果，对服务外包风险管理能力进行持续改进和优化。

4.2.2 承包方能力成熟度模型

承包方应从公司治理和风险管理、战略管理、经营状况、信誉、服务能力、服务管理、服务连续性、信息安全管理、合规管理和工具管理等方面建立服务外包风险管理能力模型规范。按照能力模型规范的要求，结合组织的具体情况进行实施，同时对建立服务外包风险管理能力模型规范的效果进行监控评估，并根据评估结果，对服务外包风险管理能力进行持续改进和优化。

4.3 评估

由评估机构依据本标准对外包行为主体（发包方、承包方）的外包风险管理能力进行独立、客观评估。

5 发包方能力成熟度规范

5.1 战略管理

5.1.1 策略管理

发包方应根据自身实际情况形成外包战略决策机制，以组织的战略目标为依据，综合风险、成本、效益等因素，制定与自身规模、市场定位相适应的服务外包策略，包括服务外包的定位、规划、模式、资源能力建设、分级管理以及供方关系管理等。

5.1.2 范围管理

发包方应确定与其风险管理水平、技术能力相适宜的服务外包范围。发包方的计划与组织、监控与评价等管理职能不宜外包。

5.1.3 需求管理

发包方应在确定服务外包范围的基础上，确定服务外包需求并进行有效管理。服务外包需求应明确服务级别。

5.2 组织与制度管理

5.2.1 组织结构

发包方应设置层级清晰的企业级的服务外包管理组织结构，包括董事会及高级管理层、外包管理层和外包执行团队三个层级。

5.2.2 管理责任

发包方应明确定义外包管理组织结构中各层级的职责。包括：

- a) 明确信息科技服务外包风险管理的最终责任，明确监督和实施管理的责任；
- b) 明确制定并监督实施信息科技服务外包战略和服务外包风险策略的责任；
明确外包管理的部门、执行团队及其外包管理角色、职责，明确有效的沟通和协作机制；
- c) 明确与发包方、承包方、第三方评估机构以及监管机构之间的沟通机制。

5.2.3 人力资源保障

发包方应根据自身外包策略和风险管理目标要求，配备足够的人力资源从事外包管理工作。

5.2.4 制度管理

发包方应建立服务外包的相关制度，制度应涵盖服务外包风险管理的各个方面，包括但不限于：

- a) 风险管理；
- b) 信息安全管理；
- c) 外包生命周期管理；
- d) 供方管理。

5.3 外包关系管理

发包方应指定专人建立并定期维护全部承包方（及其分包方）清单，并依据本标准对其实施分类分级管理，包括但不限于：

- a) 风险评估和尽职调查；
- b) 建立承包方沟通和风险监测长效机制；
- c) 建立事件响应和争议解决机制。

5.4 流程管理

5.4.1 决策流程

发包方应依据信息科技外包战略建立服务外包决策流程，内容包括外包的必要性及可行性分析、外包的风险及收益分析、评审、决策等。

5.4.2 需求管理

发包方应建立需求管理流程，内容包括需求编制、变更、评审和审批等。

5.4.3 采购流程

发包方应依据信息科技外包战略建立并优化服务外包的采购及审批流程，内容包括采购计划、采购方式、承包方遴选、采购评审和审批流程等。

5.4.4 合同管理

发包方应就所开展的服务外包活动与承包方签订书面合同或协议，明确双方的权利义务。依据具体的服务外包内容，签订服务级别协议。

发包方应建立合同管理流程，内容包括合同的谈判、审核、签订、履行和变更等。

5.4.5 执行过程管理

发包方应针对不同的外包服务内容, 建立相应的外包服务执行过程的管理流程，内容包括但不限于：

- a) 计划管理；
- b) 服务级别管理；
- c) 服务请求管理；
- d) 变更管理；
- e) 财务管理；
- f) 资源管理；
- g) 质量管理。

5.4.6 交付管理

发包方应针对不同的外包服务内容, 建立相应的外包服务交付的管理流程，内容包括但不限于：

- a) 服务级别协议（SLA）；
- b) 服务交付物管理；
- c) 服务连续性和可用性管理；
- d) 服务预算与核算；
- e) 知识产权管理；
- f) 能力管理；
- g) 服务满意度评估；
- h) 供方管理；
- i) 知识转移。

5.4.7 评价管理

发包方应建立服务外包管理的评价机制，定期对服务外包管理进行评价，并作为服务外包战略调整的依据。

发包方应制定对承包方评价的制度和流程，内容包括评价目的、评价方法、评价过程和评价结果应用，并作为承包方准入、奖惩、退出等的依据。

5.5 质量管理

发包方应建立和维护服务外包质量管理体系，根据明确的质量要求、程序和政策来编制质量管理计划、实施和维护质量管理体系。

发包方应根据信息科技外包服务需求、合同、服务水平协议等建立明确的服务质量监控指标，并进行监控。发包方应采用可实现的定量指标阐述和传达质量要求，并定期对服务外包质量、进度、成本、资源保障、沟通情况和风险等进行审计与评价，通过监控、分析和响应偏差来实现持续改进，并将结果传达给利益相关方。

5.6 风险管理

发包方应将信息科技服务外包管理纳入全面风险管理体系，应明确服务外包风险管理的主管部门，建立风险管理的制度和流程以及有效的业务连续性管理机制，定期开展外包风险管理评估和审计，对承包方应进行风险评估、审计和持续监控等措施。

5.7 信息安全管理

发包方应建立信息安全管理体系，制定和落实安全保密、信息和知识产权保护措施，明确针对服务外包以及发包方信息保护的相关要求。

对信息安全管理按照GB/T 22080-2016的要求进行，涉及服务外包的重要信息系统，按照JR/T 0071-2012的要求实行等级保护。

信息安全管理的内容包括但不限于：

- a) 安全方针；
- b) 信息安全组织；
- c) 资产管理；
- d) 人力资源安全；
- e) 物理和环境安全；
- f) 通信和操作管理；
- g) 访问控制；
- h) 信息系统获取开发和维护；

- i) 信息安全事件管理；
- j) 业务连续性管理；
- k) 符合性。

5.8 合规管理

发包方应确保服务外包遵循相关法律法规，符合行业监管要求。

5.9 工具管理

发包方宜使用一系列管理工具，以实现对服务外包的量化管理，确保实现服务外包管理目标。

6 承包方能力成熟度规范

6.1 公司治理和风险管理

承包方应建立同自身信息科技服务性质、规模相匹配的组织风险治理架构，明确董事会、高级管理层、职能部门、服务部门在风险管理中的职责分工，建立多层次、相互衔接、有效制衡的组织级风险识别、评估、监测和控制等工作机制。包括：

- a) 设立或指定信息科技服务风险管理部门和负责人；
- b) 建立和完善信息科技服务风险管理相关制度；
- c) 建立向发包方以及监管机构的信息科技服务风险定期报告机制。

6.2 战略管理

6.2.1 发展战略和业务规划

承包方应建立金融行业信息科技服务外包业务的发展战略，建立符合行业以及自身发展需求的商业目标，以指导承包业务的经营和管理，包括：

- a) 根据自身和金融发包方的发展需求、市场信息、国家及监管机构政策要求和行业自律要求等，进行战略规划，建立商业目标，制定并落实具体的实施方案；
- b) 承包方应跟踪实施方案的执行情况，评估是否能够达成商业目标；
- c) 承包方应根据自身和发包方的运营状况、市场及其他外部因素的变化，适时调整商业目标和战略规划。

6.3 经营状况

6.3.1 基本条件

承包方应具备满足承担金融信息科技服务的基本条件。

6.3.2 财务状况

承包方的财务状况应适应所要提供的服务类型，资产负债、盈利水平、现金流等财务状况良好，支持组织可持续经营和发展。

6.4 信誉

承包方应在所提供的服务领域具备良好的信誉。在规定时间内没有不良行为记录。

6.5 服务能力

6.5.1 技术能力

承包方应充分掌握从事信息科技服务所需的信息技术，能够有效进行服务交付，并有能力对技术的有效性和充分性进行管理。

6.5.2 人员能力

承包方应获得、保持并激励具备能力的员工交付信息科技服务。为实现上述目标，应建立和遵循既定的程序，包括招聘、培训、绩效评估等。

人员能力包括但不限于以下方面：

- a) 利益相关方对信息科技人员的技能和经验的满意程度；
- b) 信息科技人员参与同类信息科技服务的经验；
- c) 信息科技人员学识和相关资质获得情况。

6.5.3 资源整合能力

承包方应对所承包项目中的资源予以落实并进行有效管理，包括人员、知识、技术、财务、基础设施、供应商等资源。

6.5.4 服务案例

承包方应具备与所提供的服务相适应的成功服务案例，并实施有效的知识管理。

6.6 服务管理

6.6.1 服务交付

6.6.1.1 服务目录

承包方应建立和维护所提供服务的信息列表，包括但不限于：

- a) 根据发包方需求、市场信息以及组织自身的能力定义能够提供的服务，建立服务目录。服务目录一般包括：服务名称、服务指标、服务等级、服务时间、安全方案等；
- b) 组织应在服务目录中考虑不同发包方、不同类型的服务需求；
- c) 组织应确保服务目录的持续有效，在发包方需求、市场条件和自身能力发生变化时，对服务目录进行维护。

6.6.1.2 服务管理

服务管理包括但不限于以下内容：

- a) 需求管理：定义、分析、评审和确认服务需求，以及管理服务需求状态和优先级；
- b) 服务级别管理：定义、协商、记录并管理服务级别协议（SLA）；
- c) 合同管理：明确服务范围 and 水平，确定双方的权利和责任，避免或减少合同实施过程中的争议，规范合同签订和日常管理流程；
- d) 服务交付物管理：根据合同要求，确定服务交付物的内容、版本、验收标准等；
- e) 沟通管理：确保信息及时、准确、适当地传递给相关方，持续改善组织沟通能力；
- f) 可用性和容量管理：对所提供服务的连续性、可用性和容量进行管理的规范；
- g) 知识产权管理：对服务所涉及的知识产确认和保护等；
- h) 服务满意度评估：对所提供服务满意度的评估；
- i) 知识转移：在服务过程中，为发包方提供相关培训等知识和经验辅导活动。

6.6.1.3 服务持续改进

承包方应建立服务的持续改进机制，确保服务水平不断提高。

6.6.2 服务支持

服务支持管理中应考虑包括但不限于以下内容：

- a) 计划管理；
- b) 项目或任务管理；
- c) 变更管理；
- d) 配置管理；
- e) 知识管理；

- h) 质量管理；
- i) 沟通管理。

6.7 服务连续性

承包方应当建立同自身信息科技服务性质、规模相匹配的服务连续性管理机制，减低信息科技服务中断发生概率和由此造成的损失。要求：

- a) 明确服务连续性管理部门、岗位和责任人。其中，服务连续性管理负责人应由公司负责业务的高管担任；
- b) 应制定服务应急计划，定期更新、演练或测试服务应急计划，确保其充分性和可行性；
- c) 应针对外包人员大量流失、系统重大技术缺陷等可能引起服务中断或服务水平严重下降的场景制定相应的应急预案，并定期开展应急预案演练工作；
- d) 应配合发包方制定所承包服务相关的应急预案和演练，提前准备并维护好相关资源，确保在承包服务及相关系统出现紧急情况时，对发包方实施相关的应急预案提供充分的支持。

6.8 信息安全管理

承包方应建立信息安全管理机制，制定和落实安全保密、信息和知识产权保护措施，明确针对服务外包以及发包方信息保护的相关要求。

承包方应定期对所提供的服务涉及的信息安全管理的符合性进行评估，确保所承担服务满足信息安全管理要求。

信息安全管理应符合GB/T 22080-2016，包括但不限于以下内容：

- a) 安全方针；
- b) 信息安全组织；
- c) 资产管理；
- d) 人力资源安全；
- e) 物理和环境安全；
- f) 通信和操作管理；
- g) 访问控制；
- h) 信息系统获取开发和维护；
- i) 信息安全事件管理；

T/CCUA 004-2018

j) 业务连续性管理；

k) 符合性。

6.9 合规管理

承包方应确保服务外包活动遵循相关法律法规，确保不损害发包方及监管机构和主管部门的监管效能。

6.10 工具管理

承包方宜使用一系列管理工具，以实现对所承包服务的量化管理和目标。

第二部分：发包方成熟度分级准则

7 发包方成熟度级别概述

发包方成熟度按照从I到V级能力的演变过程，划分为如下5个级别：

第I级

发包方按照最基本的要求管理服务外包。

第II级

发包方建立了较完善的制度和文档体系。

第III级

已建立了较完善的制度流程和评价机制。

第IV级

在第III级基础上，通过量化数据来执行或辅助管理。

第V级

基于持续改进的结果及外部组织的成熟度模型，工作流程已被优化为行业优秀实践。

注：第I-V级分别对应☆、☆☆、☆☆☆、☆☆☆☆、☆☆☆☆☆。

8 第I级

8.1 战略管理

本级不包含战略管理。

8.2 组织与制度管理

8.2.1 组织结构

本级不包含组织结构管理。

8.2.2 责任体系

本级不包含责任体系管理。

8.2.3 制度管理

建立了服务外包的信息安全管理制度。

8.3 外包关系管理

本级不包含外包关系管理。

8.4 流程管理

8.4.1 需求管理

本级不包含需求管理。

8.4.2 决策流程

本级不包含决策流程。

8.4.3 采购流程

建立了通用的产品/供应商遴选、评审和审批流程。

8.4.4 合同管理

建立了合同的谈判、签订和执行流程。

8.4.5 执行过程管理

本级不包含执行过程管理。

8.4.6 交付管理

建立了对承包方服务交付的验收流程。

8.4.7 绩效考核和承包方评价

本级不包含绩效考核和承包方评价。

8.5 质量管理

建立了初步的服务外包质量管理流程和方法。

8.6 风险管理

明确了服务外包风险管理的主管部门，能够达到监管机构的风险管控要求。

8.7 信息安全管理

制定和落实了安全保密、信息和知识产权保护、信息安全等级保护等措施。

8.8 合规管理

服务外包活动按照相关法律法规和监管要求执行。

8.9 工具管理

本级不包含工具管理。

9 第 II 级

9.1 战略管理

9.1.1 策略管理

根据自身实际情况形成战略决策机制，以组织的战略目标为依据，综合风险、成本、效益等因素，制定了初步的服务外包策略。

9.1.2 范围管理

初步确定了与其风险管理水平、技术能力相适宜的服务外包活动范围。

9.1.3 需求和服务级别管理

确定了初步的服务外包需求，初步明确了各项外包服务的服务级别。

9.2 组织与制度管理

9.2.1 组织结构

设置了服务外包管理团队。

9.2.2 责任体系

服务外包管理团队中各个角色有明确的职责分工。

9.2.3 制度管理

建立了初步的服务外包实施制度和信息安全制度。

9.3 外包关系管理

本级不包含外包关系管理。

9.4 流程管理

9.4.1 需求管理

建立了服务外包需求起草、评审和审批流程。

9.4.2 决策流程

建立了基本的审批决策流程。

9.4.3 采购流程

建立了信息科技服务专有的产品/承包方的遴选、评审和审批流程。

9.4.4 合同管理

建立了合同的谈判、审核、签订和执行流程。

9.4.5 执行过程管理

建立了对承包方服务执行过程的管理流程。

9.4.6 交付管理

建立了对承包方服务交付的管理流程。

9.4.7 绩效考核和承包方评价

建立了服务外包绩效考核和承包方评价的方法和流程。

9.5 质量管理

建立了初步的服务外包质量管理流程和方法。

9.6 风险管理

明确了服务外包风险管理的主管部门，建立了风险管理的制度和流程。

9.7 信息安全管理

制定和落实了安全保密、信息和知识产权保护、信息安全等级保护措施；涉及重要信息系统的服务外包，参照JR/T 0071-2012的要求进行管理。

9.8 合规管理

服务外包活动按照相关法律法规和监管要求执行。

9.9 工具管理

本级不包含工具管理。

10 第 III 级

10.1 战略管理

10.1.1 策略管理

根据自身实际情况形成战略决策机制，以组织的战略目标为依据，综合风险、成本、效益等因素，制定了明确的服务外包策略，包括服务外包的定位、模式和供方关系管理等，形成了初步的文档。

10.1.2 范围管理

详细确定了与其风险管理水平、技术能力相适宜的服务外包活动范围。

10.1.3 需求和服务级别管理

确定了详细的服务外包需求，明确了各项外包服务的服务级别。

10.2 组织与制度管理

10.2.1 组织结构

服务外包组织结构包括董事会及高级管理层、外包管理部门、外包服务执行团队三个层次。

10.2.2 责任体系

董事会及高级管理层、外包管理部门、外包服务执行团队中各个角色有明确的职责分工。

10.2.3 制度管理

建立了服务外包实施制度、承包方管理制度、外包风险管理制度、信息安全制度、外包生命周期管理制度。

10.3 外包关系管理

建立了承包方清单，按照承包方所提供的服务，对重要、非驻场、集中式承包方进行了识别，对各类承包方制定并实施了有针对性的外包关系管理策略。

10.4 流程管理

10.4.1 需求管理

建立了服务外包需求起草、评审和审批流程，形成了完善的文档模板和优秀实践文档库。

10.4.2 决策流程

建立了服务外包可行性分析、风险分析、评审及审批决策流程，形成了完善的文档模板和优秀实践文档库。

10.4.3 采购流程

建立了信息科技服务专有的产品/承包方的遴选、评审和审批流程，形成了完善的文档模板和优秀实践文档库。

10.4.4 合同管理

建立了合同的谈判、审核、签订和执行流程，形成了完善的文档模板和优秀实践文档库。

10.4.5 执行过程管理

建立了承包方服务执行过程的管理流程，形成了完善的文档模板和优秀优秀实践文档库。

10.4.6 交付管理

建立了承包方服务交付的管理流程，形成了完善的文档模板和优秀优秀实践文档库。

10.4.7 评价管理

建立了服务外包和承包方评价的方法和流程，形成了完善的文档模板和优秀优秀实践文档库。

10.5 质量管理

建立了服务外包质量管理体系，包括：质量计划、质量保证、质量控制等。

10.6 风险管理

明确了服务外包风险管理的主管部门，建立了风险管理的制度和流程，对服务外包活动的风险进行定性分析，建立了业务连续性管理机制。

10.7 信息安全管理

制定和落实了安全保密、信息和知识产权保护和信息安全等级保护措施；参照GB/T 22080-2008的要求建立了信息安全管理体系统；涉及重要信息系统的服务外包，按照JR/T 0071-2012的要求实行等级保护并通过测评。

10.8 合规管理

服务外包活动按照相关法律法规和监管要求执行，近1年内无国家有关部门及监管相关公开处罚记录。

10.9 工具管理

应使用工具进行有效管理，并建立明确的工具使用制度。

11 第 IV 级

11.1 战略管理

11.1.1 策略管理

根据自身实际情况形成战略决策机制，以组织的战略目标为依据，综合风险、成本、效益等因素，结合服务外包管理的量化数据，制定了明确的服务外包策略，包括服务外包的定位、规划、模式、资源能力建设、分级管理以及供方关系管理等，形成了完善的文档。

11.1.2 范围管理

根据服务外包管理的量化数据，详细确定了与其风险管理水平、技术能力相适宜的服务外包活动范围。

11.1.3 需求和服务级别管理

根据服务外包管理的量化数据，确定了详细的服务外包需求，明确了各项外包服务的服务级别。

11.2 组织与制度管理

11.2.1 组织结构

服务外包组织结构包括董事会及高级管理层、外包管理部门、外包服务执行团队三个层次。

11.2.2 责任体系

董事会或授权机构、外包风险主管部门、外包管理归口部门、外包服务执行团队中各个角色有明确的职责分工。

11.2.3 制度管理

建立了服务外包实施制度、承包方管理制度、风险管理制度、质量管理制度和信息安全制度。

11.3 外包关系管理

建立并维护了全部的承包方（包括分包方和业务外包相关的信息科技服务承包方）清单，并依据本标准对其实施分类分级管理，根据外包关系管理的量化数据适时调整外包关系管理行为，包括：

- a) 风险评估和尽职调查；
- b) 建立承包方沟通和风险监测长效机制；
- c) 建立事件响应和争议解决机制。

11.4 流程管理

11.4.1 需求管理

建立了服务外包需求起草、评审和审批流程，形成了完善的文档模板和完备的优秀实践文档库。

11.4.2 决策流程

建立了服务外包可行性分析、风险分析、评审及审批决策流程，形成了完善的文档模板和完备的优秀实践文档库，根据服务外包管理的量化数据来辅助决策。

11.4.3 采购流程

建立了信息科技服务专有的产品/承包方的遴选、评审和审批流程，形成了完善的文档模板和完备的优秀实践文档库，根据服务外包管理的量化数据来辅助评选。

11.4.4 合同管理

建立了合同的谈判、风险审核、合规审核、签订和执行流程，形成了完善的文档模板和完备的优秀实践文档库。

11.4.5 执行过程管理

建立了对承包方服务执行过程的管理流程，形成了完善的文档模板和完备的优秀实践文档库，根据服务外包管理的量化数据来辅助管理。

11.4.6 交付管理

建立了对承包方服务交付的管理流程，形成了完善的文档模板和完备的优秀实践文档库。

11.4.7 绩效考核和承包方评价

建立了服务外包绩效考核和承包方评价的方法和流程，形成了完善的文档模板和完备的优秀实践文档库，根据服务外包管理的量化数据来辅助评价。

11.5 质量管理

建立了服务外包质量管理体系，包括：质量计划、质量保证、质量控制等，根据服务外包管理的量化数据来提升服务外包质量。

11.6 风险管理

明确了服务外包风险管理的主管部门，建立了风险管理的制度和流程，对服务外包活动的风险进行定量分析，建立了有效的业务连续性管理机制。

11.7 信息安全管理

制定和落实了安全保密、信息和知识产权保护、信息安全等级保护措施；参照GB/T 22080-2008的要求建立了信息安全管理体系并通过有关认证；涉及重要信息系统的服务外包，参照JR/T 0071-2012的要求实行等级保护并通过测评。

11.8 合规管理

服务外包管理基本符合相关法律法规和监管要求，近2年内无国家有关部门及监管相关公开处罚记录。

11.9 工具管理

应使用工具进行有效管理和建立明确的工具使用制度，能够通过工具进行量化分析和决策。

12 第V级

12.1 战略管理

12.1.1 策略管理

根据自身实际情况形成战略决策机制，以组织的战略目标为依据，综合风险、成本、效益等因素，结合服务外包管理的量化数据，制定了明确的服务外包策略，包括服务外包的定位、模式以及供方关系管理等，形成了完善的文档，并有持续优化机制。

12.1.2 范围管理

根据服务外包管理的量化数据，详细确定了与其风险管理水平、技术能力相适宜的服务外包活动范围，要求达到资源级，并有持续优化机制。

12.1.3 需求和服务级别管理

根据服务外包管理的量化数据，确定了详细的服务外包需求，明确了各项外包服务的级别，并有持续优化机制。

12.2 组织与制度管理

12.2.1 组织结构

服务外包组织结构包括董事会及高级管理层、外包管理部门、外包服务执行团队三个层次。

12.2.2 责任体系

董事会或授权机构、外包风险主管部门、外包管理归口部门、外包服务执行团队中各个角色有明确的职责分工。

12.2.3 制度管理

建立了服务外包实施制度、承包方管理制度、风险管理制度、质量管理制度和信息安全制度。

12.3 外包关系管理

指定专人建立并维护了全部的承包方（包括分包方和业务外包相关的信息科技服务承包方）清单，并依据本标准对其实施分类分级管理，根据外包关系管理的量化数据适时调整外包关系管理行为，并建立了持续优化机制，包括但不限于：

- a) 风险评估和尽职调查；
- b) 建立承包方沟通和风险监测长效机制；
- c) 建立事件响应和争议解决机制。

12.4 流程管理

12.4.1 需求管理

建立了服务外包需求起草、评审和审批流程，形成了完善的文档模板和完备的优秀实践文档库，并有持续优化机制。

12.4.2 决策流程

建立了服务外包可行性分析、风险分析、评审及审批决策流程，形成了完善的文档模板和完备的优秀实践文档库，根据服务外包管理的量化数据来辅助决策，并有持续优化机制。

12.4.3 采购流程

建立了信息科技服务专有的产品/承包方的遴选、评审和审批流程，形成了完善的文档模板和完备的优秀实践文档库，根据服务外包管理的量化数据来辅助评选，并有持续优化机制。

12.4.4 合同管理

建立了合同的谈判、风险审核、合规审核、签订和执行流程，形成了完善的文档模板和完备的优秀实践文档库，并有持续优化机制。

12.4.5 执行过程管理

建立了对承包方服务执行过程的管理流程，形成了完善的文档模板和完备的优秀实践文档库，根据服务外包管理的量化数据来辅助管理，并有持续优化机制。

12.4.6 交付管理

建立了对承包方服务交付的管理流程，形成了完善的文档模板和完备的优秀实践文档库，并有持续优化机制。

12.4.7 绩效考核和承包方评价

建立了服务外包绩效考核和承包方评价的方法和流程，形成了完善的文档模板和完备的优秀实践文档库，根据服务外包管理的量化数据来辅助评价，并有持续优化机制。

12.5 质量管理

建立了服务外包质量管理体系，包括：质量计划、质量保证、质量控制等，根据服务外包管理的量化数据来提升服务外包质量，并有持续优化机制。

12.6 风险管理

明确了服务外包风险管理的主管部门，建立了风险管理的制度和流程，对服务外包活动的风险进行定量分析，建立了有效的业务连续性管理机制，并有持续优化机制。

12.7 信息安全管理

制定和落实了安全保密、信息和知识产权保护措施；按照GB/T 22080-2008的要求建立了信息安全管理体系并通过有关认证，并有效实施一年以上；涉及重要信息系统的服务外包，按照JR/T 0071-2012的要求实行等级保护并通过测评。

12.8 合规管理

服务外包管理符合相关法律法规和监管要求，近5年内无国家有关部门及监管相关公开处罚记录。

12.9 工具管理

应使用工具进行有效管理和建立明确的工具使用制度，能够通过工具进行量化分析和决策，持续改进管理效率。

第三部分：承包方成熟度分级准则

13 承包方成熟度级别概述

承包方成熟度定级是根据承包方在公司治理和风险管理、战略管理、经营状况、信誉、服务能力、服务管理、服务连续性管理、信息安全管理、合规管理和工具管理等方面的情况，从低到高划分为I到V级。

第I级

承包方已初步具备提供服务外包活动的能力。

第II级

承包方在单一专业领域具备提供服务的能力。

第III级

承包方具有一定的信誉和服务能力。

第IV级

承包方已具备较好的信誉和综合服务能力。

第V级

承包方已具备与发包方持续共赢、优势互补的全面合作能力。

服务承包方成熟度评价申请组织应具备以下基本条件：

- a) 在中华人民共和国境内注册，具有独立法人地位的实体，发展历程清晰、产权关系明确；
- b) 能够独立或合作提供金融信息科技外包服务；
- c) 遵守国家有关法律、法规和条例，近一年在经营活动中没有重大违法、违规记录；
- d) 有良好的履约能力，近一年未出现过验收未获通过的项目或应由承包方承担责任的重大用户投诉；
- e) 近一年无不正当竞争行为；

- f) 能够主动接受行业自律和监督;
- g) 遵守本标准相关规定, 在成熟度定级申报和分级使用过程中诚实守信, 近一年无不良行为。

14 第 I 级

14.1 公司治理和风险管理

承包方按照《中华人民共和国公司法》、《中华人民共和国劳动合同法》等国家有关法律法规的要求, 制定了较为规范的公司章程、公司治理结构、股东会、董事会议事规则等, 明确了股东会、董事会、经理层的职责和权限。

14.2 战略管理

承包方根据自身和发包方的发展需求、市场和国家政策等, 进行战略规划, 建立与所服务行业有明确关系的经营目标。

14.3 经营状况

14.3.1 综合条件

承包方发展历程清晰、产权关系明确; 应有明确的成立时间; 在转制、更名、合并、分立等变更事项中业绩、人员、资产继承关系明确, 股权关系明确。

14.3.2 财务状况

承包方自身的财务状况应符合所要提供的服务外包业务类型。承包方近一年内主业没有出现亏损。

14.4 信誉

承包方应在所提供的服务领域具备良好的信誉。近一年内没有出现违约行为和责任事故, 没有不正当竞争行为, 包括篡改、伪造、租用或借用成熟度定级参与市场活动, 以及串通投标、低于成本的报价竞标等扰乱市场秩序的行为。

近一年内没有定级申报的不良行为; 承包方没有在定级初次申报、升级、再定级、监管评估及变更事项中的弄虚作假行为, 没有出租、出借成熟度定级的不良行为。

14.5 服务能力

14.5.1 技术能力

承包方能对主要业务领域的业务流程和特点有一定程度的熟悉，能够在发包方的明确指导下为发包方提供服务解决方案。

14.5.2 人员能力

承包方组织实施了人力资源培训计划与考核。承包方信息科技人员具备同类信息科技服务的经验不少于一年。

14.5.3 资源整合能力

承包方能够对特定的服务外包项目中的资源，包括人员、知识、技术、财务、基础设施、供应商等进行管理。

14.5.4 服务案例

本级不包含服务案例的要求。

14.6 服务管理

14.6.1 服务交付

14.6.1.1 服务目录

承包方能够根据发包方需求定义提供服务。

14.6.1.2 服务管理

承包方能够按照本标准有效实施需求管理、合同管理、服务交付物管理、沟通管理和知识转移。

14.6.1.3 服务持续改进

本级不包含服务持续改进。

14.6.2 服务支持

承包方能够按照本标准进行服务支持管理。

14.7 服务连续性管理

承包方按照发包方的要求，配合制定外包服务相关的应急预案和演练。

14.8 信息安全管理

承包方按照GB/T 22080-2008的要求对信息科技人员进行了信息安全意识培训。

14.9 合规管理

承包方确保服务外包活动遵循相关法律和规范。

14.10 工具管理

本级不包含工具使用。

15 第 II 级

15.1 公司治理和风险管理

承包方按照《中华人民共和国公司法》、《中华人民共和国劳动合同法》等国家有关法律法规的要求，制定了较为规范的公司章程、公司治理结构、股东会、董事会议事规则等，明确了股东会、董事会、经理层的职责和权限。并具备：

- a) 承包方应指定信息科技服务风险责任人；
- b) 建立信息科技服务外包风险相关的管理制度。

15.2 战略管理

具体要求如下：

- a) 承包方根据自身和发包方的发展需求、市场和国家政策等，进行战略规划，建立商业目标；
- b) 承包方部署实施方案以达成组织的商业目标。

15.3 经营状况

15.3.1 综合条件

承包方发展历程清晰、产权关系明确：企业应有明确的成立时间，在转制、更名、合并、分立等变更事项中业绩、人员、资产继承关系明确，股权关系明确。

承包方现有成熟度一级首次定级时间须满两年；或由二级降为一级的，须满六个月；或承包方参与的首个金融业信息科技服务项目合同签订时间满一年。

15.3.2 财务状况

承包方自身的财务状况应适应所要提供的服务外包业务类型。承包方近一年内主业没有出现亏损。

15.4 信誉

承包方应在所提供的服务领域具备良好的信誉。近一年内没有出现违约行为和责任事故，没有不正当竞争行为，包括篡改、伪造、租用或借用成熟度定级参与市场活动，以及串通投标、低于成本的报价竞标等扰乱市场秩序的行为。

近一年没有定级申报的不良行为：在定级初次申报、升级、再定级、监管评估及变更事项中的弄虚作假行为，出租、出借成熟度定级。

15.5 服务能力

15.5.1 技术能力

承包方在某一专业领域具备独特优势，能通过学习对主要业务领域的业务流程和特点有一定程度的熟悉，能够根据发包方的明确需求，为发包方业务目标的实现提供有价值的服务解决方案。

15.5.2 人员能力

承包方的人力资源培训计划的组织实施与考核应有记录、可核查。

根据第三方评估机构的认定，承包方信息科技人员提供同类信息科技服务的经验平均不少于两年；或者利益相关方对信息科技人员的技能和经验的满意度达到80%以上。

15.5.3 资源整合能力

承包方对特定的服务外包项目中的资源，包括人员、知识、技术、财务、基础设施、供应商等进行有效管理。承包方对资源管理进行年度评估。

15.5.4 服务案例

本级不包含服务案例的要求。

15.6 服务交付

15.6.1 服务目录

承包方应建立和维护能够提供的服务信息，要求：

- a) 承包方应根据发包方需求、市场信息以及组织自身的能力定义能够提供的服务，建立服务目录。服务目录一般包括：服务名称、服务指标、服务等级、服务时间、安全方案等；
- b) 承包方应在服务目录中考虑不同发包方、不同应用领域的服务需求。

15.6.2 服务管理

承包方按照本标准有效实施了需求管理、合同管理、服务交付物管理、沟通管理和知识转移。对服务管理进行年度评估。

15.6.3 服务持续改进

承包方对服务水平进行年度评估。

15.7 服务支持

承包方按照本标准进行服务支持管理。对服务支持管理进行年度评估。

15.8 服务连续性管理

承包方按照发包方的要求，配合制定外包服务相关的应急预案和演练。

15.9 信息安全管理

承包方按照GB/T 22080-2008的要求有效进行信息安全管理，对信息安全管理进行年度评估。

15.10 合规管理

承包方确保服务外包活动遵循相关法律和规范。

15.11 工具管理

本级不包含工具使用。

16 第 III 级

16.1 公司治理和风险管理

承包方按照《中华人民共和国公司法》、《中华人民共和国劳动合同法》等国家有关法律法规的要求，制定了较为规范的公司章程、公司治理结构、股东会、董事会议事规则等，明确了股东会、董事会、经理层的职责和权限。要求：

- a) 承包方应明确信息科技服务风险责任人及岗位职责；
- b) 具备完善的信息科技服务外包风险管理制度；
- c) 具备向发包方和监管机构的信息科技服务外包风险定期报告机制。

16.2 战略管理

具体要求：

- a) 承包方根据自身和发包方的发展需求、市场和国家政策等，进行战略规划，建立商业目标；
- b) 承包方对实施方案进行论证，确保实施方案的可行性；
- c) 承包方部署实施方案以达成组织的商业目标；
- d) 承包方根据自身和发包方的运营状况、市场及其他外部因素的变化，适时修改商业目标。

16.3 经营状况

16.3.1 综合条件

承包方发展历程清晰、产权关系明确：企业应有明确的成立时间，在转制、更名、合并、分立等变更事项中业绩、人员、资产继承关系明确，股权关系明确。

承包方现有成熟度二级，首次定级时间须满两年；或由三级降为二级的，须满六个月；或承包方参与的首个金融业信息科技服务项目合同签订时间满两年。

16.3.2 财务状况

承包方的注册资本和实收资本不少于500万，注册成立时间应不少于3年，承包方三年内主业没有出现亏损。

16.4 信誉

承包方应在所提供的服务领域具备良好的信誉。近两年没有出现违约行为和责任事故，没有不正当竞争行为，包括篡改、伪造、租用或借用成熟度定级参与市场活动，以及串通投标、低于成本的报价竞标等扰乱市场秩序的行为。

近两年没有定级申报的不良行为：在定级初次申报、升级、再定级、监管评估及变更事项中的弄虚作假行为，出租、出借成熟度定级。

16.5 服务能力

16.5.1 技术能力

承包方应具有足够的技术能力、人员队伍和设施、环境，满足外包服务的质量和安全管理要求。应建立完备的自身服务支撑知识库体系，应具有完善的运行服务管理体系，并通过行业认可的运行服务管理资质认证。机房及基础设施应达到国家电子计算机机房较高标准。

承包方应对主要业务领域的业务流程和特点有一定程度的熟悉，能够了解发包方的需求，能够为发包方业务目标的实现提供有价值的服务解决方案。

16.5.2 人员能力

承包方应有人力资源培训、考核管理制度，具有系统地对员工进行新知识、新技术以及职业道德培训的计划。

承包方的人力资源管理制度和培训计划应在实际工作中得到贯彻执行，且有记录、可核查。

根据第三方评估机构的认定，承包方信息科技人员提供同类信息科技服务的经验平均不少于三年；或者利益相关方对信息科技人员的技能和经验的满意度达到85%以上。

16.5.3 资源整合能力

承包方对特定的服务外包项目中的资源，包括人员、知识、技术、财务、基础设施、供应商等进行有效管理。承包方对资源管理进行年度评估，评估结果用于进一步改进，完善和调整资源管理。

16.5.4 服务案例

承包方近三年内完成全国性金融机构地市级分支行（或相当等级金融机构）服务外包项目一个以上。

承包方建立了发包方对其过往信息科技外包服务的满意程度的调查机制，近三年满意程度为80%以上。

16.6 服务交付

16.6.1 服务目录管理

承包方应建立和维护能够提供的服务信息，要求：

- a) 承包方应根据发包方需求、市场信息以及组织自身的能力定义能够提供的服务，建立服务目录。服务目录一般包括：服务名称、服务指标、服务等级、服务时间、安全方案等；
- b) 承包方应在服务目录中考虑不同发包方、不同应用领域的服务需求；
- c) 承包方应建立服务目录裁剪的准则；
- d) 承包方应确保服务目录的持续有效，在发包方需求、市场条件和自身能力发生变化时，应对服务目录进行更新。

16.6.2 服务管理

承包方按照本标准有效进行服务管理，对服务管理进行年度评估，并利用评估结果进一步改善和调整服务管理。

16.6.3 服务持续改进

应具有完善的质量管理体系，并通过行业认可的质量管理资质认证。

承包方对服务水平进行年度评估，评估结果用于进一步改进、完善和调整服务水平。

16.7 服务支持

承包方按照本标准有效进行服务支持活动，对服务支持活动进行年度评估，并利用评估结果进一步改善和调整服务支持活动。

16.8 服务连续性管理

承包方应当具备同自身信息科技服务性质、规模相匹配的服务连续性管理体系，减低信息科技服务中断发生概率和由此引起的损失。要求：

- a) 明确服务连续性管理部门和责任人；
- b) 应制定服务应急计划，确保其充分性和可行性；
- c) 应针对外包人员大量流失、系统重大技术缺陷等可能引起服务中断或服务水平严重下降的场景，制定相应的应急预案，并定期开展应急预案演练工作；
- d) 应配合发包方制定外包服务相关的应急预案和演练，提前准备并维护好相关资源，确保在外包服务及相关系统出现紧急情况时，对发包方实施相关的应急预案提供充分的支持。

16.9 信息安全管理

承包方应具有完善的信息安全管理体系、业务连续性管理体系，并通过行业认可的信息安全管理和业务连续性管理资质认证。

承包方按照GB/T 22080-2008的要求有效进行信息安全管理，对信息安全管理进行年度评估，并利用评估结果进一步改善和调整信息安全管理。

16.10 合规管理

承包方确保服务外包活动遵循相关法律和规范。

16.11 工具管理

应使用工具进行有效管理，并建立明确的工具使用制度。

17 第 IV 级

17.1 公司治理和风险管理

承包方按照《中华人民共和国公司法》、《中华人民共和国劳动合同法》等国家有关法律法规的要求，制定了较为规范的公司章程、公司治理结构、股东会、董事会议事规则等，明确了股东会、董事会、经理层的职责和权限。要求：

- a) 承包方应明确指定信息科技服务外包风险管理部门、岗位及责任人；
- b) 具备持续完善信息科技服务外包风险管理制度；
- c) 建立向发包方和监管机构的信息科技服务外包风险定期报告和整改落实机制。

17.2 战略管理

具体要求：

- a) 承包方根据自身和发包方的发展需求、市场和国家政策等进行战略规划，建立商业目标；
- b) 承包方就服务外包战略规划制定具体的实施方案，采用绩效管理等实施手段；
- c) 承包方对实施方案进行论证，确保实施方案的可行性；
- d) 承包方部署实施方案以达成组织的商业目标；
- e) 承包方跟踪实施方案的执行情况，评估是否能够达成商业目标；
- f) 承包方根据自身和发包方的运营状况、市场及其他外部因素的变化，适时修改商业目标。

17.3 经营状况

17.3.1 综合条件

承包方发展历程清晰、产权关系明确：企业应有明确的成立时间，在转制、更名、合并、分立等变更事项中业绩、人员、资产继承关系明确，股权关系明确。

承包方现有成熟度为三级的，三级首次定级时间须满两年；或由四级降为三级的，须满六个月。

17.3.2 财务状况

承包方的注册资本和实收资本不少于1000万，注册成立时间应不少于3年，承包方三年内主业没有出现亏损，同时利润率和利润同比保持稳定或上升。

17.4 信誉

承包方应在所提供的服务领域具备良好的信誉。近三年没有出现违约行为和责任事故，没有不正当竞争行为，包括篡改、伪造、租用或借用成熟度定级参与市场活动，以及串通投标、低于成本的报价竞标等扰乱市场秩序的行为。

近三年没有定级申报的不良行为：在定级初次申报、升级、再定级、监管评估及变更事项中的弄虚作假行为，出租、出借成熟度定级。

17.5 服务能力

17.5.1 技术能力

承包方应具有足够的技术能力、人员队伍和设施、环境，满足外包服务的质量和安全管理要求。应建立完备的自身服务支撑知识库体系，应具有完善的运行服务管理体系，并通过行业认可的运行服务管理资质认证。机房及基础设施应达到国家电子计算机机房较高标准。

承包方应对主要业务领域的业务流程和特点有一定程度的熟悉，能够了解发包方的需求，能够为发包方业务目标的实现提供有价值的服务解决方案。

承包方技术带头人具有八年及以上的行业技术背景。

17.5.2 人员能力

承包方的人力资源管理体系涵盖人力资源规划、招聘与配置、培训与开发、绩效管理、薪酬管理、劳动关系管理等主要方面。

承包方应设有人力资源管理部门，有人力资源管理制度，具有系统地对员工进行新知识、新技术以及职业道德培训的计划。

承包方的人力资源管理制度和培训计划应在实际工作中得到贯彻执行，且有记录、可核查。

根据第三方评估机构的认定，承包方信息科技人员提供同类信息科技服务的经验平均不少于四年；或者利益相关方对信息科技人员的技能和经验的满意度达到90%以上。

17.5.3 资源整合能力

承包方对特定的服务外包项目中的资源，包括人员、知识、技术、财务、基础设施、供应商等进行有效管理。承包方对资源管理进行年度评估，评估结果用于进一步改进，完善和调整资源管理。

17.5.4 服务案例

承包方近三年内完成全国性金融机构省级分支行（或相当等级金融机构）服务外包项目两个以上。

承包方建立了发包方对其过往信息科技外包服务的满意程度的调查机制，近三年满意程度为90%以上。

17.6 服务交付

17.6.1 服务目录管理

承包方应建立和维护能够提供的服务信息，要求：

- a) 承包方应根据发包方需求、市场信息以及组织自身的能力定义能够提供的服务，建立服务目录。服务目录一般包括：服务名称、服务指标、服务等级、服务时间、安全方案等；
- b) 承包方应在服务目录中考虑不同发包方、不同应用领域的服务需求；
- c) 承包方应建立服务目录裁剪的准则；
- d) 承包方应确保服务目录的持续有效，在发包方需求、市场条件和自身能力发生变化时，应对服务目录进行更新。

17.6.2 服务管理

承包方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。

承包方按照本标准有效进行服务管理，对服务管理进行年度评估，并利用评估结果进一步改善和调整服务管理。

17.6.3 服务持续改进

应具有完善的质量管理体系，并通过行业认可的质量管理资质认证。

承包方对服务水平进行年度评估，评估结果用于进一步改进、完善和调整服务水平。

17.7 服务支持

承包方按照本标准有效进行服务支持活动，对服务支持活动进行年度评估，并利用评估结果进一步改善和调整服务支持活动。

17.8 服务连续性管理

承包方应当具备同自身信息科技服务性质、规模相匹配的服务连续性管理体系，并通过了行业认可的业务连续性管理资质认证。要求：

- a) 明确服务连续性管理部门、岗位和责任人。其中，外包服务连续性管理负责人应

由公司负责外包业务的高管担任；

- b) 应制定服务应急计划，定期更新、演练或测试服务应急计划，确保其充分性和可行性；
- c) 应针对外包人员大量流失、系统重大技术缺陷等可能引起服务中断或服务水平严重下降的场景制定相应的应急预案，并定期开展应急预案演练工作；
- a) 应配合发包方制定外包服务相关的应急预案和演练，提前准备并维护好相关资源，确保在外包服务及相关系统出现紧急情况时，对发包方实施相关的应急预案提供充分的支持。

17.9 信息安全管理

承包方应具有完善的信息安全管理体系，并通过行业认可的信息安全管理资质认证。

17.10 合规管理

承包方应确保服务外包活动遵循有关法律、法规和规范。

17.11 工具管理

应使用工具进行有效管理和建立明确的工具使用制度，能够通过工具对服务管理进行量化分析和决策。

18 第V级

18.1 公司治理和风险管理

承包方按照《中华人民共和国公司法》、《中华人民共和国劳动合同法》等国家有关法律法规的要求，制定了规范完备的公司章程、公司治理结构、股东会、董事会议事规则等，明确了股东会、董事会、经理层的职责和权限。要求：

- a) 承包方应具有分工明确、相互制衡、运行高效的信息科技服务外包风险管理和审计部门、岗位及责任人；
- b) 具有完备的、行业先进、量化改进的信息科技服务外包风险管理体系；
- c) 建立了面向利益相关方的信息科技服务外包风险预警、应急、报告和整改落实机制。

18.2 战略管理

具体要求：

- a) 承包方根据自身和发包方的发展需求、市场和国家政策等进行战略规划，建立商业目标；
- b) 承包方就服务外包战略规划制定具体的实施方案，采用绩效管理等实施手段；
- c) 承包方对实施方案进行论证，确保实施方案的可行性；
- d) 承包方部署实施方案以达成组织的商业目标；
- e) 承包方跟踪实施方案的执行情况，评估是否能够达成商业目标；
- f) 承包方根据自身和发包方的运营状况、市场及其他外部因素的变化，适时修改商业目标；
- g) 承包方应根据管理的需要，将商业目标分解到业务单元，建立业务单元的商业目标。

18.3 经营状况

18.3.1 综合条件

承包方发展历程清晰、产权关系明确：企业应有明确的成立时间，在转制、更名、合并、分立等变更事项中业绩、人员、资产继承关系明确，股权关系明确。应具有信息科技风险的管理体系，有效识别、监测、评估和控制风险。

承包方现有成熟度为四级的，四级首次定级时间须满两年；或由五级降为四级的，须满六个月。

18.3.2 财务状况

承包方的注册资本和实收资本不少于1000万，注册成立时间应不少于3年，承包方三年内主业没有出现亏损，同时利润率和利润同比保持稳定或上升。

18.4 信誉

承包方应在所提供的服务领域具备良好的信誉。近三年没有出现违约行为和责任事故，没有不正当竞争行为，包括篡改、伪造、租用或借用成熟度定级参与市场活动，以及串通投标、低于成本的报价竞标等扰乱市场秩序的行为。

近三年没有定级申报的不良行为：承包方没有在定级初次申报、升级、再定级、监管评估及变更事项中的弄虚作假行为，没有出租、出借成熟度定级的不良行为。

18.5 服务能力

18.5.1 技术能力

承包方应具有足够的技术能力、人员队伍和设施、环境，满足外包服务的质量和安全管理要求。应建立完备的自身服务支撑知识库体系，应具有完善的运行服务管理体系，并通过行业认可的运行服务管理资质认证。机房及基础设施应达到国家电子计算机机房最高标准。

为支持服务交付、减小技术风险、提高技术核心竞争力，应对技术的有效性和充分性进行管理。承包方对主要业务领域的业务流程和特点有深入和长期的研究，能够较好地把握发包方的需求，能够为发包方战略和业务目标的实现提供有价值的服务解决方案。

承包方技术带头人具有十年及以上的行业技术背景。

18.5.2 人员能力

承包方的人力资源管理体系涵盖人力资源规划、招聘与配置、培训与开发、绩效管理、薪酬管理、劳动关系管理等主要方面。

承包方应设有人力资源管理部门，有人力资源管理制度，具有系统地对员工进行新知识、新技术以及职业道德培训的计划。

承包方的人力资源管理制度和培训计划应在实际工作中得到贯彻执行，且有记录、可核查。

整体人员异动率不超过10%，关键人员异动率不超过5%。

根据第三方评估机构的认定，承包方信息科技人员提供同类信息科技服务的经验平均不少于五年；或者利益相关方对信息科技人员的技能和经验的满意度达到95%以上。

18.5.3 资源整合能力

承包方对特定的服务外包项目中的资源，包括人员、知识、技术、财务、基础设施、供应商等建立了进行有效管理的机制，其管理有效。承包方对资源整合能力进行年度评估，评估结果用于进一步改进，完善和调整资源整合机制和要求。

18.5.4 服务案例

承包方近三年内完成全国性金融机构省级分支行（或相当等级金融机构）服务外包项目三个以上，其中全国性金融机构总行的服务外包项目一个以上。

承包方建立了发包方对其过往信息科技外包服务的满意程度的调查机制，近三年满意程度为95%以上。

18.6 服务交付

18.6.1 服务目录管理

承包方应建立和维护能够提供的服务信息，要求：

- a) 承包方应根据发包方需求、市场信息以及组织自身的能力定义能够提供的服务，建立服务目录。服务目录一般包括：服务名称、服务指标、服务等级、服务时间、安全方案等；
- b) 承包方应在服务目录中考虑不同发包方、不同应用领域的服务需求；
- c) 承包方应建立服务目录裁剪的准则；
- d) 承包方应确保服务目录的持续有效，在发包方需求、市场条件和自身能力发生变化时，应对服务目录进行更新。

18.6.2 服务管理

承包方按照本标准有效建立了服务管理体系和机制，并有效实施。承包方建立了对服务管理体系的年度评估机制，并利用评估结果进一步优化服务管理体系和机制。

18.6.3 服务外包持续改进

应具有完善的质量管理体系，并通过行业认可的质量管理资质认证。

承包方建立服务的持续改进机制，并对服务水平进行年度评估，评估结果用于进一步改进、完善和调整服务水平。

18.6.4 交付管理

承包方按照本标准建立了交付管理体系和机制，并有效实施。承包方建立了对交付管理的年度评估机制，并利用评估结果进一步优化交付管理体系和机制。

18.7 服务支持

承包方按照本标准建立了服务支持管理体系和机制，并有效实施。承包方建立了对服务支持管理的年度评估机制，并利用评估结果进一步优化服务支持管理体系和机制。

18.8 服务连续性管理

承包方应当具备完善的、先进的服务连续性管理体系，并通过了行业认可的业务连续性管理资质认证。

承包方按照GB/T 22080-2008的要求建立了服务连续性管理体系，通过了相关认证并有效实施一年以上。承包方建立了对服务连续性管理的年度评估机制，并利用评估结果进一步优化服务连续性管理体系和机制。

18.9 信息安全管理

承包方应具有完善的信息安全管理体系，并通过行业认可的信息安全管理和业务连续性管理资质认证。

承包方按照GB/T 22080-2008的要求建立了信息安全管理体系统，通过了相关认证并有效实施一年以上。承包方建立了对信息安全管理的年度评估机制，并利用评估结果进一步优化信息安全管理体系统，并机制。

18.10 合规管理

承包方确保服务外包活动遵循相关法律和规范。

18.11 工具管理

应使用工具进行有效管理和建立明确的工具使用制度，能够通过工具对服务进行量化分析和决策，持续改进服务效率和质量。

第四部分：评估的基本原则和流程

19 评估基本原则

19.1 评估对象

本标准的评估对象是信息科技服务外包活动的发包方和承包方。

19.2 评估依据和前提

本标准对发包方进行评级应依据本标准第二部分相关条款，从战略管理、组织与制度管理、外包关系管理、流程管理、质量管理、风险管理、信息安全管理、合规管理、工具管理等方面结合组织的具体情况进行评估，并根据评估结果，进行成熟度定级。

本标准对承包方进行评级应依据本标准第三部分相关条款，从公司治理与风险管理、战略管理、经营状况、信誉、服务管理、服务连续性管理、信息安全管理、合规管理和工具管理等方面进行评估，并根据评估结果，进行成熟度定级。

在评估前，被评估单位应已按照本标准由专业评估机构或自行开展了标准的实施工作。

19.3 评估范围

评估范围依据被评估对象所开展的服务外包活动及其定级需求所对应的本标准评估范围，评估对象的定级限于本标准评估范围内。

19.4 评估机构

评估机构应为经行业组织认可的专业的第三方评估机构。

19.5 评估人员

评估人员参与评估应受评估机构的指派，接受评估机构的管理，遵循评估机构设计的评估方法，使用评估机构的评估工具，依照评估机构确定的评估时间、评估内容和范围内对评估对象进行评估，并向评估机构提供评估报告。

评估人员应经过相关组织的专业培训合格并取得评估机构的授权方可从事评估活动，培训内容应包括本标准相关内容和有关实施细则、评估细则等。

19.6 主评估员

评估机构应指定一名主评估员负责评估的管理。其责任包括但不限于：

- a) 设计并维护一个有效的评估计划和评估范围；
- b) 沟通并协调所有的评估活动，包括评估计划、会议、与相关部门的沟通；
- c) 和评估对象召开总结会议，审阅评估结论以及建议工作；
- d) 组织编写和签署书面评估报告。

19.7 评估方法

评估过程中，评估人员根据评估对象所申报定级级别，按照本标准相应级别的要求逐项进行评估，并标明每个检查项的符合性状态。符合性状态应可为符合、不符合、待定。

- a) 如果每个检查项的状态均为符合，则评估对象通过该级别评定；
- b) 如果存在不符合项，则评估对象不通过该级别评定；
- c) 如果存在待定项，评估对象应补充材料或提供相关证明材料并参加再次评估，以确定该检查项是否符合。

20 评估流程

评估流程包括：评估准备、开场会议、现场评审、总结反馈、高级管理层会议和提交评估报告等。

20.1 定级结果报告

评估机构应在规定期间内完成定级结果报告。内容应包括并不限于：评估对象、评估范围、评估过程、评估结果、定级结果等。

评估机构应在规定时间内进行复评、修订、批准及提交定级结果报告。

20.2 定级结果分发

评估机构应将评估报告分发到评估对象处，定级结果由评估机构存档并向相关组织备

案。对于评估结果，评估机构应与评估对象建立良好的沟通机制。

21 定级的有效期

定级有效期为三年，有效期内每年应定期进行一次评审。如果发包方/承包方定级有效期满或者整体状况有较大变化时，评估机构应根据本标准给出的定级方法进行重新定级，并将定级的结果予以通报。

参 考 文 献

- [1] 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
 - [2] 银行业金融机构信息科技风险管理指引 银监发〔2009〕19号
 - [3] G7: FUNDAMENTAL ELEMENTS FOR THIRD PARTY CYBER RISK MANAGEMENT IN THE FINANCIAL SECTOR (G7:金融领域第三方网络风险管理的基本要素)
-