

ICS 35.240.40

CCS L67

T/CCUA

中国计算机用户协会团体标准

T/CCUA LX05-2020

代替T/CCUA 003-2019

金融科技外包风险管理能力

成熟度模型与评估

Risk management capability maturity model and assessment for outsourcing of
financial information technology

(征求意见稿)

(在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上)

本稿完成日期：2022年10月28日

2022-XX-XX 发布

2022-XX-XX 实施

中国计算机用户协会 发布

目 次

前言.....	错误！未定义书签。
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 能力成熟度模型.....	3
4.1 综述.....	3
4.2 发包方能力成熟度模型.....	3
4.3 承包方能力成熟度模型.....	4
5 能力成熟度评估.....	4
5.1 发包方能力成熟度评估总体要求.....	5
5.2 承包方能力成熟度评估总体要求.....	6
5.3 被评估方申报.....	7
5.4 确定评估方案.....	7
5.5 提供评估实证.....	7
5.6 评定能力成熟度等级.....	7
5.7 评价结果分析及改进.....	7
附录 A（资料性）能力框架.....	8
附录 B（规范性）能力成熟度评估规则.....	9
附录 C（规范性）能力成熟度评估表.....	20
附录 D（资料性）评估示例.....	24
参考文献.....	错误！未定义书签。

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件替代T/CCUA 003-2019《金融信息科技服务外包风险管理成熟度评估规范》，与T/CCUA 003-2019相比，除结构调整和编辑性改动外，主要技术变化如下：

- 更改了标准名称，具体修改为“金融信息科技外包风险管理能力成熟度模型与评估”；
- 增加了外包的分类分级管理，包括外包类别、特殊要求外包分类和重要性级别，增加外包服务提供商风险管理能力成熟度等级的应用方法；
- 增加了数据安全和个人信息保护的内容；
- 增加了业务连续性管理相关内容，主要增加了影响业务连续性管理的风险点，包括全球供应链风险、公共卫生突发事件风险、自然灾害等；

本文件由中国计算机用户协会归口管理。

本文件起草单位：中国计算机用户协会信息科技审计分会、招商银行股份有限公司、华夏银行股份有限公司、中治研（北京）国际信息技术研究院、中国农业发展银行、中国农业银行股份有限公司、中国银行股份有限公司、中国建设银行股份有限公司、交通银行股份有限公司、中国邮政储蓄银行股份有限公司、上海浦东发展银行股份有限公司、渤海银行股份有限公司、赣州银行股份有限公司、洛阳银行股份有限公司、九江银行股份有限公司、广州银行股份有限公司、泰安银行股份有限公司、深圳前海微众银行股份有限公司、江西裕民银行股份有限公司、开泰银行（中国）有限公司、北京农村商业银行股份有限公司、广东省农村信用社联合社、贵州省农村信用社联合社、福建省农村信用社联合社、中国人寿（集团）股份有限公司、中国人寿财产保险股份有限公司、中国银河证券股份有限公司、太平金融稽核服务（深圳）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、软通动力信息技术（集团）股份有限公司、中科软科技股份有限公司、中电科技（北京）有限公司、国家电子计算机质量监督检验中心、上海市锦天城（北京）律师事务所、深圳正一会计师事务所（特殊普通合伙）。

本文件主要起草人：李印波、韩建国、林创、孙卫东、姜健、车忠良、张正、王琰、杨晓平、刘松林、陈勤、刘剑锋、于伟琳、刘园、毛咏梅、何乃煜、李徽翡、陈致祥、戴文静、程建国、韩继炆、李鹏、颜涵、袁晟、丁伟、李海涛、刘超、罗志伟、刘天亮、班翊坤、钟锋、方立雄、尹君、伯军友、刘玲、郑良、林炳灵、何启翱、陈鑫（农）、陈鑫（中）、董俏、蔡炫楠、关竞楠、郝秀丽、邱俊、张海波、黄炬峰、

崔玉玺、黄先伟、李城漳、罗曦、王庆久、杨方、尹雪、陈群林、李海龙、魏东、陈星、陈晟、王颖、张荣、陈文超、于亚男。

本文件及其所替代文件的历次版本发布情况为：

——2019年首次发布为T/CCUA 003-2019，本次为第1次修订。

金融信息科技外包风险管理能力成熟度模型与评估

1 范围

本文件确立了金融业信息科技外包风险管理能力成熟度模型，规定了发包方和承包方能力成熟度评估的总体要求，并给出了对发包方和承包方进行外包风险管理能力成熟度评估的方法。

本文件适用于金融行业信息科技外包活动行为主体(包含发包方和承包方)的外包风险管理能力成熟度评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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

3 术语和定义

下列术语和定义适用于本文件。

3.1

金融信息科技外包 information technology outsourcing in financial industry

金融机构将原本由自身负责的信息科技活动委托给服务提供商进行处理的行为。包括：咨询规划类、开发测试类、运行维护类、安全服务类、业务支持类等。

3.2

金融信息科技外包风险 information technology outsourcing risk in financial industry

金融机构在信息科技外包过程中的诸多不确定性可能导致的战略、声誉、合规等风险，包括但不限于：科技能力丧失、业务中断、数据泄露、丢失和篡改、资金损失、服务水平下降等影响。

3.3

发包方 outsourcing contractee

信息科技外包服务的需方。

3.4

承包方 outsourcing contractor

信息科技外包服务的提供商，简称服务提供商。

3.5

金融信息科技外包风险管理能力 Risk management capability of financial information technology outsourcing

金融机构为有效应对信息科技外包风险,保障组织战略、管理、服务目标有效达成的能力。

3.6

能力构造 construction of capability

与金融信息科技外包风险管理能力有关的且存在结构联系的概念,对组织信息科技外包风险管理的某一局部能力的认识和概括。

[来源: T/CCUA 012-2021, 3.1.3]

3.7

能力域 capability area

一组相关能力项的集合。

3.8

能力项 capability item

一个单项能力。

[来源: GB/T 33136-2016, 3.1.6]

3.9

管理能力成熟度 management capability maturity

金融机构针对信息科技外包风险管理开展的相关的管理活动及其体现的成熟度。本文件中以能力项涵盖了能力建设、能力检验、能力维持、能力优化等表现及评价,以成熟度等级反映金融机构的外包风险管理能力。

3.10

管理能力成熟度评估对象 management capability maturity assessment object

管理能力成熟度评估采用能力成熟度模型及能力项进行评估定级,具体的评估对象主要包括金融机构信息科技外包风险管理活动相关的发包方、承包方主体管理制度、流程和结果记录等。

[来源: T/CCUA 012-2021, 3.1.5]

3.11

发包方能力成熟度 capability maturity of the contractee

体现发包方对信息科技外包管理和风险控制能力程度的一种综合指标。

3.12

承包方能力成熟度 capability maturity of the contractor

体现承包方的信息科技服务承包实现和风险控制能力程度的一种综合指标。

3.13

服务管理 service management

为满足业务需求对服务进行的管理。

[来源：GB/T 24405.1-2009，2.14]

3.14

业务连续性管理 business continuity management

识别对组织的潜在威胁以及这些威胁一旦发生可能对业务运行带来的影响的一整套管理过程。该过程为组织建立有效应对威胁的自我恢复能力提供了框架，以保护关键相关方的利益、声誉、品牌和创造价值的活动。

[来源：ISO 22301-2019，3.4]

4 能力成熟度模型

4.1 综述

金融信息科技外包风险管理能力成熟度模型包含发包方能力成熟度模型和承包方能力成熟度模型。能力构成见附录A。

4.2 发包方能力成熟度模型

发包方能力可分解为外包管理的规范性、风险控制和成效控制三个方面，即3个能力域。其中规范性能力域（D1）包含组织（D1/P1）、制度（D1/P2）、流程（D1/P3）、系统（D1/P4）4个能力项，风险控制能力域（D2）包含网络安全和数据安全（D2/P1）、连续性（D2/P2）、产权（D2/P3）、合规（D2/P4）4个能力项、成效控制能力域（D3）包含成本（D3/P1）、质量（D3/P2）、效率（D3/P3）3个能力项，共11个能力项。每个能力项分为1-5个成熟度等级：起始级（1级）、发展级（2级）、稳健级（3级）、优秀级（4级）和卓越级（5级），如图1所示：

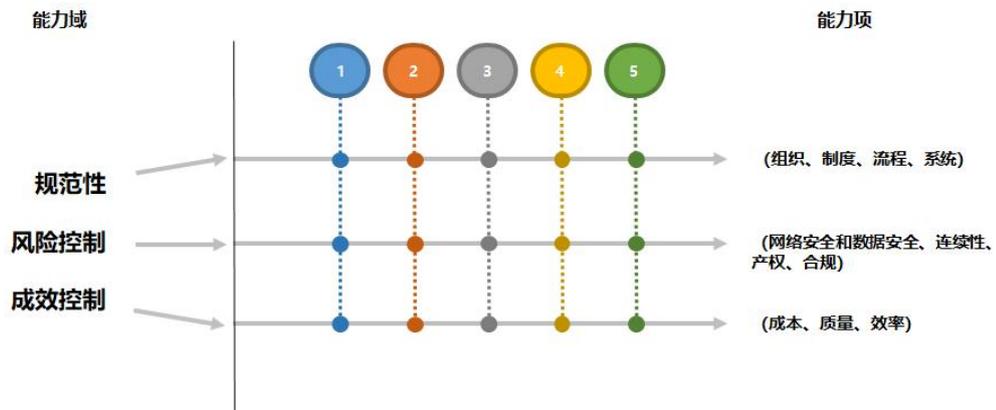


图1 发包方能力成熟度模型

4.3 承包方能力成熟度模型

承包方能力可分解为专业技术能力、服务交付能力和企业经营能力三个方面，即3个能力域。其中专业技术能力域（D4）包含技术资质（D4/P1）、软件著作权/专利（D4/P2）、人才结构（D4/P3）3个能力项，服务交付能力域（D5）包含服务体系（服务能力、服务改进、质量管理、连续性管理）（D5/P1）、服务案例（D5/P2）、网络安全和数据安全保障能力（D5/P3）、系统支持（D5/P4）4个能力项，企业经营能力域（D6）包含企业规模（D6/P1）、财务状况（D6/P2）、经营方向（D6/P3）、市场份额（D6/P4）4个能力项，共11个能力项。每个能力项都分为5个成熟度等级：起始级（1级）、发展级（2级）、稳健级（3级）、优秀级（4级）和卓越级（5级），如图2所示：

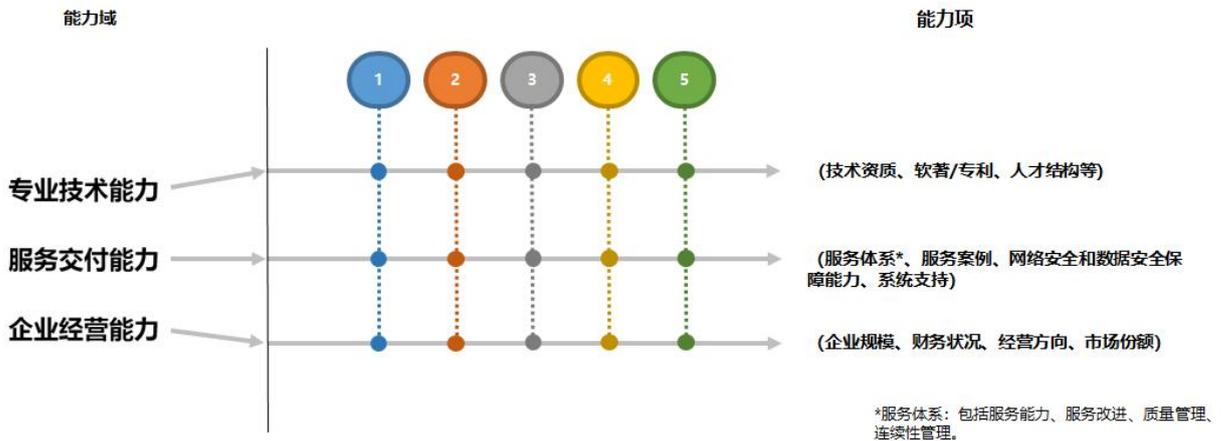


图2 承包方能力成熟度模型

5 能力成熟度评估

5.1 发包方能力成熟度评估总体要求

5.1.1 发包方能力成熟度等级

发包方能力成熟度划分为5个等级，见图3。发包方能力成熟度等级表示发包方外包风险管理能力所达到的水平，高级别的能力成熟度等级要求覆盖低级别等级的全部要求。

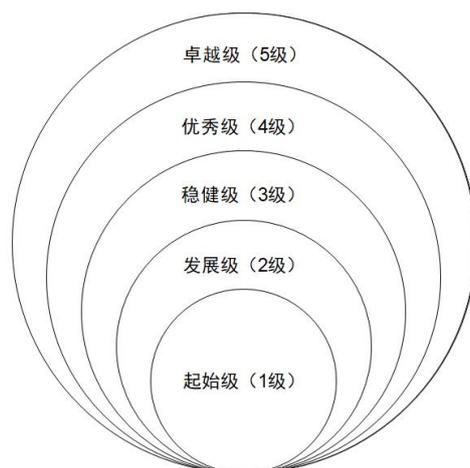


图3 能力成熟度等级

发包方能力成熟度等级对应不同的管理水平：

- a) 起始级（1级）：具有基本的金融信息科技外包风险管理制度。对外包风险的管控主要依赖自身当前拥有的资源和手段、相关人员的个人能力。
- b) 发展级（2级）：建立了较完善的组织职能、制度和流程体系。外包风险管理能力在机制、资源、手段及人员能力方面已具有常态化运作性。
- c) 稳健级（3级）：已建立了较完善的制度流程和评价机制。组织具有完整的金融信息科技外包风险管理相关制度和规划，基本满足监管、国家标准规范要求。常态化的手段和机制保障相关措施落实，为应对可能发生的金融信息科技外包风险，在机制、资源、手段及人员能力方面具有充分的准备和管理活动记录。
- d) 优秀级（4级）：在第3级基础上，通过量化数据来执行或辅助管理。组织具备完善的金融信息科技外包风险管理体系，满足监管、国家标准规范要求。实现书面化管理，借助审查、考核等有效措施，确保相关工作的严格执行，为应对可能发生的金融信息科技外包风险，在机制、资源、手段及人员能力方面具有充分的准备和管理活动记录，建立了演练、记录评审等评估评价机制，通过模型化、指标化等量化手段监测和持续改进工作效能。

- e) 卓越级（5级）：基于持续改进的结果及外部组织的外包风险管理能力成熟度模型，工作流程已被优化为行业优秀实践。组织具有完备有效并能够持续优化的金融信息科技外包风险管理体系，充分满足相关监管、国家标准规范要求，形成了较高的机构自有标准或规范。实现了系统化管理和考核确保相关措施及时执行，应用模型化、指标化等量化手段监测和持续改进工作效能，为应对可能发生的金融信息科技外包风险，在机制、资源、手段及人员能力方面具有完备的措施，具有持续改进以追求更佳的应急处置成效，建立了有效的风险控制机制。

5.1.2 发包方能力成熟度评估规则

发包方能力成熟度评估规则按附录B表B1执行。

5.2 承包方能力成熟度评估总体要求

5.2.1 承包方能力成熟度的等级

承包方的金融信息科技外包服务能力成熟度划分为5个等级，见图3。每个成熟度等级表明当前组织金融信息科技外包服务能力所达到的水平，高级别的服务能力成熟度等级要求覆盖低级别成熟度的全部要求。

不同能力成熟度等级对应不同的金融信息科技外包服务水平：

- a) 起始级（1级）：承包方已初步具备提供服务外包活动的的能力，在组织发生金融信息科技服务外包风险时，相关服务的维持或恢复以及风险应对，主要取决于自身当前拥有的资源和手段、相关人员的个人能力。
- b) 发展级（2级）：承包方在某些领域具备提供服务的能力。为应对可能发生的金融信息科技服务外包风险，在机制、资源、手段及人员能力方面具有基础性准备。
- c) 稳健级（3级）：承包方具有一定的信誉和服务能力。组织具有完整的金融信息科技外包服务相关制度和规划，基本满足监管、国家标准规范要求。通过书面化等手段和机制保障相关措施落实，为应对可能发生的金融信息科技服务外包风险，在机制、资源、手段及人员能力方面具有充分的准备和管理活动记录。
- d) 优秀级（4级）：承包方已具备较好的信誉和综合服务能力。组织具备完善的金融信息科技外包服务体系，满足监管、国家标准规范要求。实现了书面化、审查、考核等有效措施确保相关工作严格执行，为应对可能发生的金融信息科技服务外包风险，在机制、资源、手段及人员能力方面具有充分的准备和管理活动记录，建立了演练、记录评审等评估评价机制，通过模型化、指标化等量化手段监测和持续改进工作效能。

e) 卓越级（5级）：承包方已具备与发包方持续融合优势互补的全面合作能力。组织具有完备有效并能够持续优化的金融信息科技外包服务体系，充分满足相关监管、国家标准规范要求，形成了较高的机构自有标准或规范。实现了系统化管理和考核确保相关措施及时执行，应用模型化、指标化等量化手段监测和持续改进工作效能，为应对可能发生的金融信息科技服务外包风险，在机制、资源、手段及人员能力方面具有完备的措施，具有持续改进以追求更佳的应急处置成效，建立了有效的风险控制机制。

5.2.2 承包方能力成熟度评估规则

承包方能力成熟度评估规则见附录B表B2。

5.3 被评估方申报

发包方：申报方提出申请，申请的内容应包括申请评估的目标级别。

承包方：申报方提出申请，申请内容包括所申报的目标类型（咨询规划类、开发测试类、运行维护类、安全服务类、业务支持类），申请评估的目标级别。

5.4 确定评估方案

评估方应首先确定能力成熟度评价方案，其要素包括：能力成熟度评估对象、评估目标、范围、评估范围内能力域及能力项的评估标准。

评估工作应依据评价目标确定评估范围，评估范围应包含一个或多个完整的能力域，细化映射到主要的评估对象。

5.5 提供评估实证

评估方应在能力成熟度评估范围内制定调研问卷及调阅提纲，被评估机构回答问卷内容，并提供佐证资料；评估方通过调阅相关记录文档、角色访谈、演练观察、实地考察等方式核实相关内容形成评估实证。

5.6 评定能力成熟度等级

评估方评定金融信息科技外包风险管理能力成熟度等级应包括：

- a) 将被评估机构的评价实证映射至图1（发包方）或图2（承包方）对应的能力项；
- b) 按照附录B表B1（发包方）或附录B表B2（承包方）能力评估细则对能力项进行评定，并确定组织能力成熟度等级，将评估实证说明材料按照附录C进行记录。。

评估结果应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确定最终的能力成熟度等级，具体示例见附录D。

5.7 评价结果分析及改进

被评估机构对评估结果进行差距分析及改进，明确组织未来的信息科技外包风险管理发展路径。

附录 A

(资料性)

能力框架

表 A 能力框架 (第 1 页/共 1 页)

能力	能力域	能力项	能力项类型
发包方能力	D1: 规范性	P1: 组织	原则性
		P2: 制度	原则性
		P3: 流程	非原则性
		P4: 系统	非原则性
	D2: 风险控制	P1: 网络安全和数据安全	原则性
		P2: 连续性	原则性
		P3: 产权	非原则性
		P4: 合规	原则性
	D3: 成效控制	P1: 成本	非原则性
		P2: 质量	非原则性
P3: 效率		非原则性	
承包方能力	D4: 专业技术能力	P1: 技术资质	非原则性
		P2: 软件著作权/专利	非原则性
		P3: 人才结构	非原则性
	D5: 服务交付能力	P1: 服务体系 (服务能力、服务改进、质量管理、连续性管理)	非原则性
		P2: 服务案例	非原则性
		P3: 网络安全和数据安全保障能力	原则性
		P4: 系统支持	非原则性
承包方能力	D6: 企业经营能力	P1: 企业规模	非原则性
		P2: 财务状况	非原则性
		P3: 经营方向	非原则性
		P4: 市场份额	非原则性

附录 B

(规范性)

能力成熟度评估规则

表 B1 发包方能力成熟度评估规则 (第 1 页/共 4 页)

能力项编号	能力项名称	能力项类型	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
			起始级	发展级	稳健级	优秀级	卓越级
D1/P1	组织	原则性	组织中设立了外包管理的岗位(可兼岗),有专门的组织职责,实施外包风险管控	组织中设立了外包管理专职岗位,明确管理范围和职责,其中外包风险管理设立了专职岗位	(1) 组织中建立了结构层级、职责清晰的协同管理组织机构 (2) 建立了外包活动全生命周期管理 (3) 应建立外包项目管理、外包人员管理、服务提供商管理、采购/合同管理、外包风险管理岗位	(1) 外包管理组织机构实现外包活动全生命周期管理 (2) 设立了组织级机构和岗位 (3) 建立了外包活动的量化数据收集机制,形成了数据基线	(1) 自上而下的外包管理组织架构,组织架构基于外包量化数据可以快速调整、持续调优,不断推进外包活动的精细化管理 (2) 良好的组织架构和组织调整制度促进组织外包管理能力成熟度的提升
D1/P2	制度	原则性	组织初步建立了总体的外包战略和风险策略,并制定了相应的管理制度、规范。制度规范试行阶段	(1) 建立了比较完善的外包活动全生命周期的管理规范、制度,并正式发文全部项目遵照执行 (2) 应建立外包项目管理、外包人员管理、服务提供商管理、外包风险管控、网络安全和数据安全管理制度	(1) 建立自上而下的全面的外包管理体系,从决策层的外包管理战略目标、外包规划,到各部门/专岗的制度,制度具有可操作性,囊括外包活动全生命周期管理规范、指南、模板 (2) 应建立外包分类、外包风险管控、外包业务连续性管理制度	(1) 建立外包管理数据量化指标库,持续追踪数据的变化,并基于数据分析的基础上推进外包管理制度的不断完善 (2) 应建立知识产权管理、知识转移管理、集中度管理制度	(1) 形成定期更新制度的机制,并随着新技术、新管理、科技战略持续优化 (2) 建立组织级优秀实践库 应建立外包战略、项目后评价、外包关系管理制度
D1/P3	流程	非原则性	组织初步建立外包活动流程,能确保项目完成	(1) 应建立专业的外包活动流程,流程正式发布并且所有项目遵照执行 应建立外包项目立项、结项流程,外包驻场人员进场、离场流程,服务提供商准入、退出流程	(1) 应建立完善的外包活动流程,流程可以高效的辅助外包项目管理,流程要求已全部落实到流程中并不断调优 应建立外包决策流程,外包风险、网络安全和数据安全事件处理流程	(1) 应建立更加完善的外包活动流程,并建立度量与分析机制,能够推动流程的优化 应建立外包成本估算流程	(1) 流程应随组织的业务发展、研发技术、管理模式的创新做出更新 (2) 应建立高度成熟的自动化流程,流程流转高效,且流程流转时效能够进行度量,并不断调优

表 B1 发包方能力成熟度评估规则（第 2 页/共 4 页）

能力项编号	能力项名称	能力项类型	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
			起始级	发展级	稳健级	优秀级	卓越级
D1/P4	系统	非原则性	此级别不作要求	系统实现了外包项目基本管理流程，外包人员的信息登记。	<p>(1) 系统实现了外包项目生命周期全流程的管理，外包驻场人员的管理，服务提供商信息</p> <p>(2) 应包括外包项目需求、立项审批、验收、结项，外包人员进场、考勤、离场管理功能。</p>	<p>(1) 系统能实现外包项目生命周期全流程的管理，外包驻场人员的管理，服务提供商信息</p> <p>(2) 系统能提供数据统计、分析、汇总功能，能提供数据用于外包风险的监控。包括：服务提供商管理、统计报表、基线发布</p>	<p>(1) 系统能实现外包项目生命周期全流程的管理，外包驻场人员的管理，服务提供商信息</p> <p>(2) 系统能提供数据统计、分析、汇总功能，能提供数据用于外包管理的持续优化</p> <p>(3) 系统你实现项目后评价</p>
D2/P1	网络安全和数据安全	原则性	有基本的网络安全、数据安全规定和管理措施	<p>(1) 建立了外包网络安全、数据安全规范，落实到日常工作中，并实施检查</p> <p>(2) 合同包含网络安全和数据安全约定、消费者权益保护约定、外包人员驻场安全规定</p>	<p>(1) 发布了外包网络安全、数据安全规范，落实到日常工作中，并定期检查、审计的机制</p> <p>(2) 合同包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心和数据安全要求，以及包括制度、机构、人员等运维管理；驻场服务安全培训和考试；服务提供商保密协议</p>	<p>(1) 发布了外包网络安全、数据安全规范，并将安全要求融入到外包活动的流程和操作规范中，形成了适用的监测指标用于日常监测，并建立了定期检查、审计的机制</p> <p>(2) 能定期提交外包网络安全、数据安全报告</p>	<p>(1) 发布了外包网络安全、数据安全规范，并将安全要求融入到外包活动的流程和操作规范中，参与外包管理的员工养成了安全意识，并有定期检查、审计、持续改进的机制</p> <p>(2) 能定期提出外包网络安全、数据安全提升规划</p>
D2/P2	连续性	原则性	建立基本的服务连续性管理机制，识别服务连续性风险	组织发布服务连续性管理规范，在合同中有明确的服务连续性应急管理方案	<p>组织发布了服务连续性管理规范，落实到外包项目和服务提供商管理中。包括：合同中断及变更约定、服务提供商服务中断或服务水平严重下降应急预案、</p>	<p>(1) 通过了行业认可的服务连续性管理资质认证，组织发布了完善的服务连续性管理体系，落实到外包项目和服务提供商管理中</p> <p>(2) 建立了适用的监测指标用于日常风险监测，做到识别、跟踪和处置</p>	<p>(1) 通过了行业认可的服务连续性管理资质认证，组织发布了完善的服务连续性管理体系，并落实到外包项目和服务提供商管理中</p> <p>(2) 建立了对服务连续性管理的定期监测和年度评估机制，并利用监测指标和评估结果进一步优化服务连续性管理体系和机制</p>

表 B1 发包方能力成熟度评估规则（第 3 页/共 4 页）

能力项编号	能力项名称	能力项类型	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
			起始级	发展级	稳健级	优秀级	卓越级
D2/P3	产权	非原则性	外包活动中相关信息和知识产权归属权以及允许服务提供商使用内容及范围有明确要求	建立了知识产权管理规范，服务外包活动按照相关规定执行	(1) 建立了针对知识产权事件的确认、审批，以及侵权事件的处理的管理流程 (2) 形成了完善的文档模板	(1) 建立了针对知识产权事件的确认、审批，以及侵权事件的处理的管理流程 (2) 形成了完善的文档模板和优秀实践文档库，根据服务外包管理的量化数据来辅助管理	(1) 建立了针对知识产权事件的确认、审批，以及侵权事件的处理的管理流程 (2) 形成了完善的文档模板和优秀实践文档库，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
D2/P4	合规	原则性	(1) 服务外包活动按照相关法律法规和监管要求执行 (2) 有基本的外包活动合规管理规定和措施	遵照法律法规和监管要求建立了比较完善的外包活动合规管理规定和措施，服务外包活动按照相关规定执行	(1) 遵照法律法规和监管要求建立了外包活动合规要求识别、评估与处置、检查与回顾的管理制度与流程 (2) 形成了完善的文档模板并有效落实 (3) 近 1 年内无国家有关部门及监管相关公开处罚记录	(1) 遵照法律法规和监管要求建立了较完善的外包活动合规要求识别、评估与处置、检查与回顾的管理制度与流程 (2) 形成了较完善的文档模板和优秀实践文档库，根据服务外包管理的量化数据来辅助管理 (3) 近 2 年内无国家有关部门及监管相关公开处罚记录	(1) 遵照法律法规和监管要求建立了完备的外包活动合规要求识别、评估与处置、检查与回顾的管理制度与流程 (2) 形成了完备的文档模板和优秀实践文档库，根据服务外包管理的量化数据有效辅助管理，持续优化机制有效 (3) 近 4 年内无国家有关部门及监管相关公开处罚记录
D3/P1	成本	非原则性	此级别不作要求	可根据项目经验、市场询价等方法进行项目成本估算	可根据项目经验、市场询价、功能点、测试案例等方法，进行项目成本估算，项目结项后有项目成本核算机制	(1) 建立了组织级项目估算量化体系，指导外包项目立项时进行工程造价的成本估算，项目结项后，有成本核算机制 建立了人力成本基线、功能点/测试案例/其他成本基线、生产效率基线	(1) 建立了完备的组织级项目估算量化体系，有效指导外包项目工程造价的成本估算 (2) 能够根据市场变化持续优化成本，成本核算机制有效

表 B1 发包方能力成熟度评估规则（第 4 页/共 4 页）

能力项编号	能力项名称	能力项类型	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
			起始级	发展级	稳健级	优秀级	卓越级
D3/P2	质量	非原则性	初步制定外包项目质量管理流程和管控方法	(1) 建立了外包质量管理规范, 包含外包项目质量、人员质量、服务提供商质量的管控措施	(1) 建立了外包质量全面管理规范, 包含外包质量管控流程、措施、监测方法 (2) 建立了项目质量目标、质量管控措施; 外包人员资质要求、准入措施; 服务提供商准入标准、准入控制措施、服务提供商/产品/解决方案选型机制、服务评价和退出机制	(1) 制定了较完善的外包质量全面管理规范, 包含外包质量管控流程、措施、监测方法 (2) 建立了外包质量指标体系	(1) 制定了完备的外包质量全面管理规范, 包含量化外包质量管控流程、措施、监测方法 (2) 建立外包质量指标体系, 包括: 缺陷密度、系统可用率、故障解决率、故障响应时间、故障解决时间、延期率、人员本科率、人员异动率、人员流失率、违规数 (3) 有定期回检质量数据并改进的机制, 组织级度量数据不断调优, 外包质量管理数据呈上升趋势
D3/P3	效率	非原则性	此级别不作要求	对外包活动中的关键数据进行收集并分析	制定了与效率相关的管理规范, 包含研发、测试、运维等方面的效率的管理要求	(1) 建立了组织级不同类型项目的效率指标, 作用于外包项目立项决策 (2) (2) 建立了平均每人天产出的功能点/用户体验或其他可量化指标、代码行、测试案例等分析数据	(1) 建立了全面外包效率监控指标体系 (2) 能定期回检效率数据并改进的机制, 组织级度量数据不断调优, 效率指标呈上升趋势

(共 11 项, 评定级别至少须通过 9 项, 且未通过项不能为原则性能力项, 且未通过项达到目标级别的前一级要求)

表 B2 承包方能力成熟度评估规则（第 1 页/共 7 页）

能力项编号	能力项名称	能力项类型	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
			起始级	发展级	稳健级	优秀级	卓越级
D4/P 1	技术 资质	非原 则性	此级别不作要求	(1) 咨询规划类： 此级别不作要求 (2) 开发测试类： 软件企业认证 (3) 运行维护类： 此级别不作要求 (4) 安全类：CCRC 信息安全服务资质 认证 (5) 业务支持类： 无附加要求	(1) 高新企业认证，国家 或地方高新技术企业证书 (2) 咨询规划类：无附加 要求 (3) 开发测试类：附加要 求软件企业认证 (4) 运行维护类：无附加 要求 (5) 安全类：附加要求 CCRC 信息安全服务资质认证 (6) 业务支持类：无附加 要求	(1) 高新企业认证，国 家高新技术企业证书，满 一年 (2) 咨询规划类：无附 加要求 (3) 开发测试类：附加 要求软件企业认证 (4) 运行维护类：无附 加要求 (5) 安全类：附加要求 CCRC 信息安全服务资质 认证 (6) 业务支持类：无附 加要求	(1) 高新企业认证，国家高 新技术企业证书，持续满三 年 (2) 咨询规划类：无附加要 求 (3) 开发测试类：附加要求 软件企业认证 (4) 运行维护类：无附加要 求 (5) 安全类：附加要求 CCRC 信息安全服务资质认证 (6) 业务支持类：无附加要 求
D4/P 2	软件 著作 权/ 专利	非原 则性	在所申请类别相关专 业技术领域获得 2 个 以上行业相关软件著 作权登记证书	(1) 在所申请类别相关专 业技术领域获得 1 个以上发 明型专利或 3 个以上实用新 型专利 (2) 拥有行业相关软 件著作权登记证书 4 个以上 (3) 技术创新和研 发投入不低于上一 财年总收入的 5%	(1) 在所申请类别相关专 业技术领域获得 2 个以上发 明型专利或 3 个以上实用新 型专利 (2) 拥有行业相关软 件著作权登记证书 6 个以上 (3) 建立了完备的自身服 务支撑知识库体系 (4) 技术创新和研发投入 应不低于上一财年总收入 的 10%或大于 250 万	(1) 在所申请类别相关 专业技术领域获得 2 个以 上发明型专利或 4 个以上 实用新型专利 (2) 且拥有行业相关软 件著作权登记证书 8 个以 上 (3) 建立了完备的自身 服务支撑知识库体系 (4) 技术创新和研发投 入应不低于上一财年总 收入的 15%或大于 500 万	(1) 在所申请类别相关专 业技术领域获得 3 个以上发 明型专利或 5 个以上实用新 型专利 (2) 拥有行业相关软件著 作权登记证书 10 个以上 (3) 建立了完备的自身服 务支撑知识库体系 (4) 技术创新和研发投入应 不低于上一财年总收入 的 20%或大于 800 万

表 B2 承包方能力成熟度评估规则（第 2 页/共 7 页）

能力项编号	能力项名称	能力项类型	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
			起始级	发展级	稳健级	优秀级	卓越级
D4/P3	人才结构	非原则性	<p>(1) 本科及以上学历员工占比 60%以上</p> <p>(2) 信息技术人员占比不低于 60%</p>	<p>(1) 本科及以上学历员工占比不低于 60%</p> <p>(2) 信息技术人员占比不低于 60%</p> <p>(3) 整体人员异动率不超过 20%，关键人员异动率不超过 15%</p> <p>(4) 建立了教育、培训机制</p>	<p>(1) 本科及以上学历员工占比 80%以上，达到中级职称或具备中级职称能力与经验水平员工占比 5%以上</p> <p>(2) 信息技术人员占比不低于 65%</p> <p>(3) 整体人员异动率不超过 20%，关键人员异动率不超过 15%</p> <p>(4) 通过金融信息科技员工教育资质认证员工占比 15%以上，如金融从业方面的资质认证或学历学位证明，金融科技方面的资质认证或学历学位证明</p> <p>(5) 建立了教育、培训机制</p> <p>(6) 咨询规划类：附加要求通过金融信息科技员工教育资质认证员工占比 30%以上</p>	<p>(1)本科及以上学历员工占比 85%以上，达到中级职称或具备中级职称能力与经验水平员工占比 10%以上</p> <p>(2)信息技术人员占比不低于 70%</p> <p>(3)整体人员异动率不超过 15%，关键人员异动率不超过 10%</p> <p>(4)通过金融信息科技员工教育资质认证员工占比 30%以上，如金融从业方面的资质认证或学历学位证明，金融科技方面的资质认证或学历学位证明</p> <p>(5)教育、培训机制运行有效，并为之提供了必要的资源投入，为多个重点金融机构提供可持续、稳定专业的外包服务</p> <p>(6)咨询规划类：附加要求通过金融信息科技员工教育资质认证员工占比 50%以上</p>	<p>(1)本科及以上学历员工占比 90%以上，达到中级职称或具备中级职称能力与经验水平员工占比 15%以上</p> <p>(2)信息技术人员占比不低于 75%。</p> <p>(3)整体人员异动率不超过 15%，关键人员异动率不超过 5%</p> <p>(4)通过金融信息科技员工教育资质认证员工占比 50%以上，如金融从业方面的资质认证或学历学位证明，金融科技方面的资质认证或学历学位证明</p> <p>(5)教育、培训机制能持续有效运行，资源投入充分，并与所服务金融机构的战略相匹配，为多个有行业影响力的重要金融机构提供可持续、稳定专业的外包服务</p>

表 B2 承包方能力成熟度评估规则（第 3 页/共 7 页）

能力项编号	能力项名称	能力项类型	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
			起始级	发展级	稳健级	优秀级	卓越级
D5/P 1	服务体系（服务能力、服务改进、质量管理）	非原则性	此等级对该项不作要求	<p>(1) 具备服务质量管理制度</p> <p>(2) 符合信息科技风险评估和审计管理要求</p> <p>(3) 具有系统运维服务管理制度</p> <p>(4) 具有服务连续性相关制度,对连续性管理需求进行了初步评估,制定了服务连续性计划;具有充足的人力资源开展相关工作,且初步明确了应急处置流程</p> <p>(5)通过其他资质认证,如 CMMI、敏捷、精益等。参考以下标准: 开发测试类: CMMI、敏捷、精益、ISTQB 软件测试资质认证等 运行维护类: ISO20000、ITSS 运维标准(运维服务能力成熟度模型)等 安全服务类: ISO27001 等</p>	<p>(1)具备较完善的质量管理体系,并通过业界公认较为权威的质量管理资质认证,例如质量标准认证 ISO9001/ISO20000、等级保护 3 级</p> <p>(2)具备较完善的服务连续性管理体系,对连续性管理需求进行了较为充分的评估,制定了服务连续性计划,内容要素完整;具有充足的人力资源开展相关工作,且明确了各类服务中断事件的应急处置流程,建立了服务中断事件原因调查与分析机制</p> <p>(3)具备较完善的系统运维服务管理体系,并通过业界公认较为权威的运行服务管理资质认证</p> <p>(4)具备信息科技风险评估和审计管理制度</p>	<p>(1)具备完善的质量管理体系,并通过业界公认较为权威的质量管理资质认证,如质量标准认证 ISO9001/ISO20000、等级保护 3 级</p> <p>(2)具有完善的系统运维服务管理体系,并通过业界公认较为权威的运行服务管理资质认证</p> <p>(3)具备较完善的服务连续性管理体系,对连续性管理需求进行了充分的评估,制定了服务连续性计划,内容要素完整且与业务影响分析、风险评估、业务回复策略等工作成果完全一致;具有充足的人力资源开展相关工作,且明确了各类服务中断事件的应急处置流程,全面涵盖了事件的前期处置、评估与报告、应急组织、决策与指挥、复原等环节,建立了服务中断事件原因调查与分析机制,能够对事件原因进行深入的调查和分析,并对相关问题进行改进;制定了服务应急计划,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;并通过业界公认较为权威的服务连续性管理资质认证</p>	<p>(1)具有完善的质量管理体系,并通过业界公认较为权威的质量管理资质认证,例如质量标准认证 ISO9001/ISO20000、等级保护 3 级</p> <p>(2)具有完善的系统运维服务管理体系,并通过业界公认较为权威的运行服务管理资质认证</p> <p>(3)具备完善的服务连续性管理体系,对连续性管理需求进行了充分的评估,制定了服务连续性计划,内容要素完整且与业务影响分析、风险评估、业务回复策略等工作成果完全一致;具有充足的人力资源开展相关工作,且明确了各类服务中断事件的应急处置流程,全面涵盖了事件的前期处置、评估与报告、应急组织、决策与指挥、复原等环节,建立了服务中断事件原因调查与分析机制,能够对事件原因进行深入的调查和分析,并对相关问题进行改进;制定了服务应急计划,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;并通过业界公认较为权威的服务连续性管理资质认证</p>

表 B2 承包方能力成熟度评估规则（第 4 页/共 7 页）

能力项编号	能力项名称	能力项类型	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
			起始级	发展级	稳健级	优秀级	卓越级
D5/P 1	服务体系（服务能力、服务改进、质量管理）	非原则性			<p>(5) 通过其他资质认证，如 CMMI 三级等，或获得行业相关资质的中级别认证。参考以下标准： 开发测试类：CMMI、敏捷、精益、ISTQB 软件测试资质认证等 运行维护类：ISO20000、ITSS 运维标准（运维服务能力成熟度模型）等 安全服务类：ISO27001 等</p>	<p>并通过业界公认较为权威的服务连续性管理资质认证 (4) 具备信息科技风险评估和审计管理体系 (5) 通过其他资质认证，如 CMMI 四级，或获得行业相关资质的高级别认证。参考以下标准： 开发测试类：CMMI、敏捷、精益、ISTQB 软件测试资质认证等 运行维护类：ISO20000、ITSS 运维标准（运维服务能力成熟度模型）等 安全服务类：ISO27001 等</p>	<p>(4) 具备完善的信息科技风险评估和审计管理体系 (5) 建立有效的服务管理体系和机制，并有效实施，同时有评估机制，持续优化服务管理体系和机制 (6) 通过其他资质认证，如 CMMI 五级，或获得行业相关资质的最高级别认证。参考以下标准： 开发测试类：CMMI、敏捷、精益、ISTQB 软件测试资质认证等 运行维护类：ISO20000、ITSS 运维标准（运维服务能力成熟度模型）等 安全服务类：ISO27001 等</p>
D5/P 2	服务案例	非原则性	<p>本级对服务案例不作要求</p>	<p>(1) 承包方近三年内完成全国性金融机构地市级分支行（或相当等级机构）服务外包项目 2 个以上 (2) 近三年客户平均满意度，达 6 分以上（按照 NPS-净推荐值评估机制执行）</p>	<p>(1) 承包方近三年内完成全国性金融机构地市级分支行（或相当等级机构）服务外包项目 5 个以上 (2) 近三年客户平均满意度，达 7 分以上（按照 NPS-净推荐值评估机制执行）</p>	<p>(1) 承包方近三年内完成全国性金融机构省级分支行（或相当等级机构）服务外包项目 8 个以上 (2) 近三年客户平均满意度，达 8 分以上（按照 NPS-净推荐值评估机制执行）</p>	<p>(1) 承包方近三年内完成全国性金融机构省级分支行（或相当等级机构）服务外包项目 12 个以上 (2) 近三年客户平均满意度，达 9 分以上（按照 NPS-净推荐值评估机制执行）</p>

表 B2 承包方能力成熟度评估规则（第 5 页/共 7 页）

能力项编号	能力项名称	能力项类型	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
			起始级	发展级	稳健级	优秀级	卓越级
D5/P 3	网络安全和数据安全保障能力	原则性	<p>(1) 承包方制定并落实了有关知识产权的管理措施,能够确保承包服务无知识产权侵权行为或产权纠纷</p> <p>(2) 承包方应确保外包服务活动遵循相关法律和规范。确保不损害发包方及监管机构和主管部门的监管效能</p> <p>(3) 承包方按照 GB/T 22080-2016 及后续国家标准的要求对参与信息科技外包服务活动的人员进行了网络安全、数据安全意识培训</p>	<p>(1)承包方制定并落实了知识产权相关制度、方法和流程,确保所提供的外包服务无知识产权侵权行为或产权纠纷</p> <p>(2)承包方应确保外包服务活动遵循相关法律和规范。确保不损害发包方及监管机构和主管部门的监管效能</p> <p>(3) 承包方按照 GB/T 22080-2016 及后续国家标准的要求有效进行网络安全、数据安全,对网络安全、数据安全管理体系进行年度评估</p>	<p>(1) 承包方制定并落实了知识产权相关制度、方法和流程,确保所提供的外包服务无知识产权侵权行为或产权纠纷</p> <p>(2) 承包方应确保外包服务活动遵循相关法律和规范,确保不损害发包方及监管机构和主管部门的监管效能</p> <p>(3) 承包方应具有完善的网络安全、数据安全管理体系,按照 GB/T 22080-2016 及后续国家标准的要求对网络安全、数据安全管理体系进行年度评估,并利用评估结果持续改进网络安全、数据安全管理体系</p>	<p>(1) 承包方制定并落实了知识产权管理制度、方法和流程,并为之提供了必要的资源投入,以确保所提供的外包服务无知识产权侵权行为或产权纠纷</p> <p>(2) 承包方应确保外包服务活动遵循有关法律、法规和标准,确保不损害发包方及监管机构和主管部门的监管效能</p> <p>(3) 承包方应具有完善的网络安全、数据安全管理体系,并通过行业认可的网络安全、数据安全管理体系,按照 GB/T 22080-2016 及后续国家标准的要求对网络安全、数据安全管理体系进行年度评估,并利用评估结果持续改进网络安全、数据安全管理体系</p>	<p>(1) 承包方确保服务外包活动遵循相关法律和规范,确保不损害发包方及监管机构和主管部门的监管效能。近 5 年内无国家有关部门、行业监管以及金融业客户的相关公开处罚记录</p> <p>(2) 承包方应具有完善的 CCRC 信息安全服务资质认证管理体系,并通过行业认可的 CCRC 信息安全服务资质认证</p> <p>(3) 承包方按照 GB/T 22080-2016 及后续国家标准的要求建立了网络安全、数据安全管理体系,通过了相关认证并有效实施一年以上。承包方建立了对网络安全、数据安全管理体系的年度评估机制,并利用评估结果进一步优化网络安全、数据安全管理体系和机制</p>
D5/P 4	系统支持	非原则性	本级对系统支持不作要求	具有匹配交付服务的线上系统管理工具	具有匹配交付服务的线上系统管理工具,从合规和效率上提升交付服务效率和满意度	在主营业务上,普及了匹配交付服务的线上系统管理工具,从合规和效率上提升交付服务质量、效率和满意度	在主营业务上,普及了具有匹配交付服务的线上系统管理工具,从合规和效率上提升交付质量、服务效率和满意度,系统可提供数据给决策层优化服务、改进企业管理

表 B2 承包方能力成熟度评估规则（第 6 页/共 7 页）

能力项编号	能力项名称	能力项类型	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
			起始级	发展级	稳健级	优秀级	卓越级
D6/P 1	企业规模	非原则性	此级别不作要求	供职工规模，以社保缴存记录为准 咨询规划类：不少于 30 人 开发测试类：不少于 50 人 运行维护类：不少于 50 人 安全服务类：不少于 30 人 业务支持类：不少于 50 人	供职工规模，以社保缴存记录为准 咨询规划类：不少于 50 人 开发测试类：不少于 200 人 运行维护类：不少于 100 人 安全服务类：不少于 50 人 业务支持类：不少于 100 人	供职工规模，以社保缴存记录为准 咨询规划类：不少于 100 人 开发测试类：不少于 500 人 运行维护类：不少于 250 人 安全服务类：不少于 100 人 业务支持类：不少于 250 人	供职工规模，以社保缴存记录为准 咨询规划类：不少于 200 人 开发测试类：不少于 800 人 运行维护类：不少于 400 人 安全服务类：不少于 200 人 业务支持类：不少于 400 人
D6/P 2	财务状况	非原则性	(1) 自身的财务状况符合所提供的服务外包业务类型的要求 (2) 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	(1) 自身的财务状况应适应所提供的服务外包业务类型 (2) 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 (3) 前一年营业收入达到 600 万或人均产值达 30 万元，且所申请类别的收入占比不小于 50%	(1) 注册资本和实缴资本不少于 500 万，注册成立时 间应不少于 3 年，承包方一 年内主营业务没有出现亏 损 (2) 前一自然年营业收入 达到 5000 万或人均产值达 50 万元，且单一客户收入 小于 50%，且所申请类别的 收入占比不小于 40%	(1) 注册资本和实缴资本 不少于 2000 万，注册 成立时间应不少于 3 年， 承包方三年内主营业务 没有出现亏损，同时利润 率和利润同比保持稳定 或上升 (2) 前一自然年营业收 入达到 1.5 亿，且单一客 户收入小于 40%，且所申 请类别的收入占比不小 于 30%	(1) 注册资本和实缴资本 不少于 5000 万，注册成 立时间应不少于 5 年， 承包方三年内主营业务 没有出现亏损，同时利 润率和利润同比保持 稳定或上升 (2) 前一自然年营业收 入达 3 亿元，且单一客 户收入占比不小于 20%

表 B2 承包方能力成熟度评估规则（第 7 页/共 7 页）

能力项编号	能力项名称	能力项类型	第 1 级	第 2 级	第 3 级	第 4 级	第 5 级
			起始级	发展级	稳健级	优秀级	卓越级
D6/P3	经营方向	非原则性	此级别不作要求	企业主营业务，在市场上具备以下任一特征： a. 高精尖领域 b. 技术含量非高精尖，但市场需求量大	企业主营业务，在市场上具备以下任一特征： a. 高精尖领域 b. 技术含量中等，但市场需求量很大 c. 技术含量较低，市场需求巨大	企业主营业务，在市场上具备以下任一特征： a. 高精尖领域，市场潜力大 b. 技术含量中等，但市场需求量很大 c. 技术含量较低但竞争力强，市场需求巨大	企业主营业务，在市场上具备以下任一特征： a. 高精尖领域，市场潜力大 b. 技术含量中等，但市场需求量很大 c. 技术含量较低但竞争力强，市场需求巨大
D6/P4	市场份额	非原则性	此级别不作要求	所申请类别的服务中的全国性金融机构地市级分支行（或相当等级金融机构）客户数量，大于等于 2 家（以商务合同为准）	所申请类别的服务中的全国性金融机构地市级分支行（或相当等级金融机构）客户数量，大于等于 5 家（以商务合同为准）	所申请类别的服务中的全国性金融机构地市级分支行（或相当等级金融机构）客户数量，大于等于 8 家（以商务合同为准）	所申请类别的服务中的全国性金融机构地市级分支行（或相当等级金融机构）客户数量，大于等于 12 家（以商务合同为准）

（共 11 项，评定级别至少须通过 9 项，且未通过项不能为原则性能力项，且未通过项达到目标级别的前一级要求）

附录 C

(规范性)

能力成熟度评估表

表 C1 发包方能力成熟度评估表 (第 1 页/共 2 页)

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级 审议结果
D1/P1	组织	原则性	1 级要求 -xxx 2 级要求 -xxx 3 级要求 -xxx 4 级要求 -xxx 5 级要求 -xxx	被评估方已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	xx 制度, xx 规范等		5	XXX	5
D1/P2	制度	原则性							
D1/P3	流程	非原则性							
D1/P4	系统	非原则性							
D2/P1	网络安全和数据安全	原则性							
D2/P2	连续性	原则性							
D2/P3	产权	非原则性							
D2/P4	合规	原则性							
D3/P1	成本	非原则性							
D3/P2	质量	非原则性							
D3/P3	效率	非原则性							

表 C1 发包方能力成熟度评估表（第 2 页/共 2 页）

定级结果					
申报定级级别		评估时间			
被评估单位		审议时间			
定级结论	经评估, XXX 机构满足 XXX 级别相关要求, 金融科技外包风险管理能力成熟度级别(发包方) 达到 XXX 级别。				
审议小组		签字		日期	
<p>备注：评估等级分别为 1-5 级。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（评估更高级别要求时，应将所有更低级别要求作为前置条件），并标明每个能力项的符合性状态。符合性状态应可为符合、不符合、待定。</p> <p>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；</p> <p>b) 如果存在不符合项小于或等于两项，且不为原则项，则评估对象通过该级别评定；否则，则评估对象不通过该级别评定；</p> <p>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。</p>					

表 C2 承包方能力成熟度评估表（第 1 页/共 2 页）

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级审议结果
D4/P1	技术资质	非原则性							
D4/P2	软件著作权/专利	非原则性							
D4/P3	人才结构	非原则性							
D5/P1	服务体系 (服务能力、服务改进、质量管理、连续性管理)	非原则性							
D5/P2	服务案例	非原则性							
D5/P3	网络安全和数据安全保障能力	原则性							
D5/P4	系统支持	非原则性							
D6/P1	企业规模	非原则性							
D6/P2	财务状况	非原则性							
D6/P3	经营方向	非原则性							
D6/P4	市场份额	非原则性							

表 C2 承包方能力成熟度评估表（第 2 页/共 2 页）

定级结果					
申报定级级别			评估时间		
被评估单位			审议时间		
定级结论	经评估，XXX 机构满足 XXX 级别相关要求，金融信息科技外包风险管理能力成熟度级别（承包方）达到 XXX 级别。				
审议小组		签字		日期	
<p>备注：评估等级分别为 1-5 级。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（评估更高级别要求时，应将所有更低级别要求作为前置条件），并标明每个能力项的符合性状态。符合性状态应可为符合、不符合、待定。</p> <p>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；</p> <p>b) 如果存在不符合项小于或等于两项，且不为原则项，则评估对象通过该级别评定；否则，则评估对象不通过该级别评定；</p> <p>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。</p>					

附录 D

(资料性)

评估示例

表 D1：发包方能力成熟度评估示例（第 1 页/共 6 页）

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级 审议结果
D1/P1	组织	原则性	3 级要求-组织中建立了结构层级、职责清晰的协同管理组织机构，进行外包活动全生命周期管理。至少包括以下专职岗位：外包项目管理、外包人员管理、服务提供商管理、采购/合同管理、外包风险管理 4 级要求-外包管理组织机构在实现外包活动全生命周期管理的同时，设立了组织级机构和岗位，建立机制收集外包活动的量化数据，并形成数据基线。	被评估方在组织中已建立结构层次、职责清晰的协同管理组织机构，有专职的外包风险管理团队，专职的外包项目和人员管理团队，专职的采购/合同管理团队，兼职的服务提供商管理团队，已初步构建了外包活动全生命周期管理，但未形成组织级的外包管理数据采集和发布机制。	《**银行外包风险管理办法》、《**银行**外包管理团队职责和分工》、《**银行外包管理过程指引》	已满足 3 级要求，有专门的外包管理相关组织架构和流程，但未建立组织级的外包管理数据基线，未能满足 4 级要求。	3 级	XXX	3 级
D1/P2	制度	原则性	2 级要求-建立了比较完善的外包活动全生命周期的管理规范、制度，并正式发文全部项目遵照执行。 包括：外包项目管理、外包人员管理、服务提供商管理、外包风险管理、网络安全和数据安全管理 3 级要求-建立自上而下的全面的外包管理体系，从决策层的外包管理战略目标、外包规划，到各部门/专岗的制度，制度具有可操作性，囊括外包活动全生命周期管理规范、指南、模板。包括：外包分类、外包风险管理、外包连续性管理	被评估方在组织中已建立自上而下的全面的外包管理体系，外包管理各方面制度涵盖外包项目管理、人员管理、服务提供商管理、外包风险管理、网络安全和数据安全管理等方面，并在制度要求下制定了相应的操作流程，但制度较为陈旧，未能根据监管、市场等要素的变化及时进行调整和完善，可操作性不佳。	《**银行外包风险管理办法》、《**银行外包管理过程指引》	已满足 2 级要求，外包管理各方面制度较完善，但制度较为陈旧，未能根据监管、市场等要素的变化及时进行调整和优化，可操作性不佳。未能完全满足 3 级要求。	2 级	XX X	2 级

表 D1：发包方能力成熟度评估示例（第 2 页/共 6 页）

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级 审议结果
D1/P 3	流程	非原则性	3 级要求-建立了完善的外包活动流程，流程可以高效的辅助外包项目管理，流程要求已全部落实到流程中并不断调优包括：外包决策流程，外包风险、网络安全和数据安全事件处理流程 4 级要求-建立了更加完善的外包活动流程，并建立度量与分析机制，以推动流程的优化。包括：外包成本估算流程	被评估方在组织中已建立完善的外包活动流程，覆盖外包项目、外包人员、外包服务提供商管理过程，并在外包风险管理、网络安全和数据安全时间处理上也进行了有力的支撑，但在流程优化上较为被动，评估周期内只因审计问题进行了一次优化，组织级的外包度量和分析机制欠缺	《**银行外包风险管理办法》、 《**银行外包管理过程指引》、 《**银行外包人员管理指南》、 《**银行服务提供商管理指南》、 《**银行网络安全和数据安全事件处理指南》	已满足 3 级要求，外包管理各方面流程较完善，但流程优化上还需要重点关注，应推动组织及时进行流程优化，未建立组织级的外包流程监控和完善机制，未能满足 4 级要求	3 级	XX X	3 级
D1/P 4	系统	非原则性	3 级要求-系统实现了外包项目生命周期全流程的管理，外包驻场人员的管理，服务提供商信息。包括：包括：外包项目需求、立项审批、验收、结项，外包人员进场、考勤、离场 4 级要求-系统能实现外包项目生命周期全流程的管理，外包驻场人员的管理，服务提供商信息。系统提供数据统计、分析、汇总功能，能提供数据用于外包风险的监控。包括：服务提供商管理、统计报表、基线发布	被评估方在组织中已基本实现外包流程电子化，但分布于各个职能系统中，比如外包项目在项目管理系统中进行流转，流程与行内项目基本一致，加入了外包项目特有的合同验收等环节，人员管理系统在 HR 系统中完成，与自有人员基本一致，服务提供商管理流程在采购系统中完成，缺少组织级的外包管理数据和流程的监控	**银行项目管理系统、 **银行人员管理系统、 **银行采购管理系统	已满足 3 级要求，已有相关系统对外包管理流程进行支持，但缺少组织级的外包管理数据和流程的监控，未能满足 4 级要求	3 级	XX X	3 级

表 D1：发包方能力成熟度评估示例（第 3 页/共 6 页）

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级 审议结果
D2/P 1	网络安全和 数据安全	原则性	3 级要求-组织发布了外包网络安全和数据安全管理规范，落实到日常工作中，并有定期检查、审计的机制。包括：1、物理安全、数据安全，网络安全、操作安； 2、驻场服务安全培训和考试 3、服务提供商保密协议 4 级要求-组织发布了外包网络安全和数据安全管理规范，并将安全要求融入到外包活动的流程和操作规范中，形成了适用的监测指标用于日常监测，并建立了定期检查、审计的机制。包括：定期外包网络安全和数据安全报告	被评估方已根据自身实际情况组织发布了外包网络安全和数据安全管理规范，并将安全要求融入到外包活动的流程和操作规范中，形成了适用的监测指标用于日常监测，并建立了定期检查、审计的机制。包括：合同包含网络安全和数据安全约定、消费者权益保护约定、外包人员驻场安全规定；物理安全、数据安全，网络安全、操作安全；驻场服务安全培训和考试；服务提供商保密协议等	《外包网络安全和数据安全管理规范》、《外包人员驻场管理规范》、合同模板及历史合同样本	已满足 3 级要求，且相关外包网络安全和数据安全管理规范已将安全要求融入到外包活动的流程和操作规范中，但未建立定期检查、审计的机制，因此不满足 4 级要求	3 级	XX X	3 级
D2/P 2	连续性	原则性	5 级要求-通过了行业认可的服务连续性管理资质认证，组织发布了完善的服务连续性管理体系，并落实到外包项目和服务提供商管理中。建立了对服务连续性管理的定期监测和年度评估机制，并利用监测指标和评估结果进一步优化服务连续性管理体系和机制	被评估方获得了 ISO22301 业务连续性管理体系认证 (BCMS) 证书，组织发布了完善的服务连续性管理体系，并落实到外包项目和服务提供商管理中。建立了对服务连续性管理的定期监测和年度评估机制，并利用监测指标和评估结果进一步优化服务连续性管理体系和机制	《业务连续性管理体系认证 (BCMS) 证书》、历史合同样本、《服务连续性管理规范》、《服务提供商管理规范》、《服务连续性监测报告》	被评估方满足第 5 级的所有要求	5 级	XX X	5 级

表 D1：发包方能力成熟度评估示例（第 4 页/共 6 页）

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级 审议结果
D2/P3	产权	非原则性	4 级要求-建立了针对知识产权的确认、审批，以及侵权事件的处理的管理流程，形成了完善的文档模板和优秀实践文档库，根据服务外包管理的量化数据来辅助管理； 5 级要求-建立了针对知识产权的确认、审批，以及侵权事件的处理的管理流程，形成了完善的文档模板和优秀实践文档库，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	被评估方建立了针对知识产权的确认、审批，以及侵权事件的处理的管理流程，形成了完善的文档模板和优秀实践文档库，根据服务外包管理的量化数据来辅助管理。	《知识产权管理规范》及相关文档知识库系统、服务外包管理相关数据报表	被评估方已满足 4 级要求，但是相关的规范并没有形成持续的优化机制	4 级	XX X	4 级
D2/P4	合规	原则性	3 级要求-遵照法律法规和监管要求建立了外包活动合规要求识别、评估与处置、检查与回顾的管理制度与流程，形成了完善的文档模板并有效落实。近 1 年内无国家有关部门及监管相关公开处罚记录 4 级要求-遵照法律法规和监管要求建立了外包活动合规要求识别、评估与处置、检查与回顾的管理制度与流程，形成了完善的文档模板和优秀实践文档库，根据服务外包管理的量化数据来辅助管理。近 2 年内无国家有关部门及监管相关公开处罚记录	被评估方遵照法律法规和监管要求建立了外包活动合规要求识别、评估与处置、检查与回顾的管理制度与流程，形成了完善的文档模板并有效落实。近 4 年内无国家有关部门及监管相关公开处罚记录	《IT 服务外包管理规范》、相关管理文件及模板、近五年该机构的国家有关部门及监管相关公开处罚记录调阅	被评估方满足 3 级要求，建立了相关的制度流程以及完善的文档模板，且近四年内无国家有关部门及监管相关公开处罚记录。但相关制度流程未形成优秀实践文档库，因此未满足 4 级要求	3 级	XX X	3 级
D3/P1	成本	非原则性	3 级要求-可根据项目经验、市场询价、功能点、测试案例等方法，进行项目成本估算，项目结项后有项目成本核算机制。 4 级要求-建立了组织级项目估算量化体系，指导外包项目立项时进行工程造价的成本估算，项目结项后，有成本核算机制。包括：人力成本基线、功能点/测试案例/其他成本基线、生产效率基线	被评估方进行项目成本估算的工具主要有市场询价、测试案例、过往经验等。项目结项后有核算机制	《外包项目流程管理办法》、《xx 年度项目回检记录》	被评估方满足 3 级要求	3 级	XX X	3 级

表 D1：发包方能力成熟度评估示例（第 5 页/共 6 页）

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级 审议结果
D3/P2	质量	非原则性	2 级要求-对外包活动中的关键数据进行收集并分析 3 级要求-制定了与效率相关的管理规范,规范包含研发、测试、运维等方面的效率的管理要求	被评估方对外包活动中的关键数据有收集和分析的常规机制,但未在相关的管理规范中对研发、测试、运维等不同方面提出匹配的效率要求	《外包项目流程管理办法》、《外包项目质量管理办法》、《xx 年度项目回检记录》、《服务提供商绩效与服务提升管理办法》	被评估方已满足 2 级要求,但未细化落实不同类型外包活动的管理指标	2 级	XX X	2 级
D3/P3	效率	非原则性	3 级要求-制定了全面的外包质量管理规范,规范包含外包质量管控流程、措施、监测方法。包括:项目质量目标、质量管控措施;外包人员资质要求、准入措施;服务提供商准入标准、准入控制措施、服务提供商/产品/解决方案选型机制、服务评价和退出机制 4 级要求-制定了全面的外包质量管理规范,规范包含外包质量管控流程、措施、监测方法。建立外包质量指标体系。包括:(例)缺陷密度、系统可用率、故障解决率、故障响应时间、故障解决时间、延期率、人员本科率、人员异动率、人员流失率、违规数等	被评估方指定了全面的外包质量管理规范,包括质量目标和措施、服务提供商准入退出机制和服务质量评价机制	《外包项目流程管理办法》、《外包项目质量管理办法》、《xx 年度项目回检记录》、《服务提供商绩效与服务提升管理办法》	被评估方满足 3 级要求	3 级	XX X	3 级

表 D1：发包方能力成熟度评估示例（第 6 页/共 6 页）

定级结果				
申报定级级别	3 级	评估时间	2022/3/19	
被评估单位	XXX 机构	审议时间	2022/3/20	
定级结论	XXX 机构本次申报级别为 3 级，“制度”以及“质量”两个能力项等级结果为 2 级，但由于这两项都不是原则性能力项，其他能力项评估结果均满足 3 级相关要求。 经评估，XXX 机构本次申报的金融信息科技外包风险管理能力成熟度级别（发包方）达到 3 级。			
审议小组	XXX 综合审议小组	签字	日期	2022/3/20
<p>备注：评估等级分别为 1-5 级。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（评估更高级别要求时，应将所有更低级别要求作为前置条件），并标明每个能力项的符合性状态。符合性状态应可为符合、不符合、待定。</p> <p>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；</p> <p>b) 如果存在不符合项小于或等于两项，且不为原则项，则评估对象通过该级别评定；否则，则评估对象不通过该级别评定；</p> <p>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。</p>				

表D2：承包方能力成熟度评估示例（第1页/共6页）

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级 审议结果
D4/P 1	技术资质	非原创性	5级要求-高新企业认证，国家高新技术企业证书，持续满三年 咨询规划类：无附加要求 开发测试类：附加要求软件企业认证 运行维护类：无附加要求 安全服务类：附加要求 CCRC 信息安全服务资质认证 业务支持类：无附加要求	被评估方已获得国家高新技术企业证书，持续满三年，且此次申请类别为开发测试类，已通过软件企业认证	《国家高新技术企业证书》、软件企业相关认证证明材料	已满足5级要求，申请类别为开发测试类，已通过国家相关部门的软件企业认证并获得国家高新技术企业持续满三年	5级	XX X	5级
D4/P 2	软件著作权/专利	非原创性	3级要求-在所申请类别相关专业技术领域获得1个以上发明型专利或3个以上实用新型专利，且拥有行业相关软件著作权登记证书6个以上。建立了完备的自身服务支撑知识库体系。技术创新和研发投入应不低于上一财年总收入的10%或大于250万 4级要求-在所申请类别相关专业技术领域获得2个以上发明型专利或4个以上实用新型专利，且拥有行业相关软件著作权登记证书8个以上。建立了完备的自身服务支撑知识库体系。技术创新和研发投入应不低于上一财年总收入的15%或大于500万	被评估方拥有行业相关软件著作权证书45个，发明型专利1个。已建立起完备的知识库体系，研发投入900多万	行业相关软件著作权证书、专利证书、近三年财务报表、《XXX知识库管理体系》	已满足3级要求，申请类别为开发测试类，发明专利未达到2个，未满足4级要求	3级	XX X	3级

表 D2：承包方能力成熟度评估示例（第 2 页/共 6 页）

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级审议结果
D4/P 3	人才结构	非原则性	<p>3 级要求-本科及以上学历员工占比 80%以上，中级职称以上员工占比 5%以上。信息技术人员占比不低于 65%。整体人员异动率不超过 20%，关键人员异动率不超过 15%。通过金融信息科技员工教育资质认证员工占比 15%以上，如金融从业方面的资质认证或信息技术方面的资质认证</p> <p>咨询规划类：附加要求通过金融信息科技员工教育资质认证员工占比 30%以上。</p> <p>4 级要求-本科及以上学历员工占比 85%以上，中级职称以上员工占比 10%以上。信息技术人员占比不低于 70%。整体人员异动率不超过 15%，关键人员异动率不超过 10%。通过金融信息科技员工教育资质认证员工占比 30%以上，如金融从业方面的资质认证或信息技术方面的资质认证</p> <p>咨询规划类：附加要求通过金融信息科技员工教育资质认证员工占比 50%以上。</p>	<p>被评估方本科及以上学历员工占比 90%以上，中级职称以上员工占比 5%，信息技术人员占比 80%，上一年度人员异动率 10%，关键人员异动率 3%，有 50%的员工具有金融信息科技相关学历证书或接受过相关培训教育并通过资质认证</p>	<p>在职人员清单，包含学历、职称、专业、资质认证情况等；上一年度离职人员清单，包含人员所属岗位级别；人员岗位级别管理体系</p>	<p>已满足 3 级要求，但由于中级职称以上员工占比低于 10%，未满足 4 级要求</p>	3 级	XX X	3 级

表 D2：承包方能力成熟度评估示例（第 3 页/共 6 页）

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级审议结果
D5/P1	服务体系（服务能力、服务改进、质量管理、连续性管理）	非原则性	<p>3 级要求-具备较完善的质量管理体系，并通过业界公认较为权威的质量管理资质认证，例如质量标准认证 ISO9001/ISO20000、等级保护 3 级。</p> <p>具备较完善的业务服务连续性管理体系，对连续性管理需求进行了较为充分的评估，制定了服务连续性计划，内容要素完整；具有充足的人力资源开展相关工作，且明确了各类服务中断事件的应急处置流程，建立了服务中断事件原因调查与分析机制。并具备较完善的系统运维服务管理体系，并通过业界公认较为权威的运行服务管理资质认证。具备信息科技风险评估和审计管理制度。</p> <p>其他资质认证，如 CMMI 三级。获得行业相关资质的中级别认证。</p> <p>参考标准： 开发测试类：CMMI、敏捷、精益、ISTQB 软件测试资质认证等 运行维护类：ISO20000、ITSS 运维标准（运维服务能力成熟度模型）等 安全服务类：ISO27001 等</p>	<p>被评估方具备较完善的质量管理体系，具备较完善的业务服务连续性管理体系，对连续性管理需求进行了较为充分的评估，制定了服务连续性计划，内容要素完整；具有充足的人力资源开展相关工作，且明确了各类服务中断事件的应急处置流程，建立了服务中断事件原因调查与分析机制。并具备较完善的系统运维服务管理体系，并通过业界公认较为权威的运行服务管理资质认证。具备信息科技风险评估和审计管理制度。通过了 ISO 质量体系认证、ITSS 认证、CMMI3 认证</p>	<p>《XXX 质量管理体系》、《业务服务连续性管理体系》、《应急处理预案》、《系统运维服务管理体系》、ISO 质量体系认证证书、ITSS 认证证书、CMMI3 认证证书</p>	<p>已满足 3 级要求</p>	3 级	XX X	3 级

表 D2：承包方能力成熟度评估示例（第 4 页/共 6 页）

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级 审议结果
D5/P 2	服务案例	非原则性	4 级要求-承包方近三年内完成全国性金融机构省级分支行（或相当等级机构）服务外包项目 8 个以上。近三年客户平均满意度，达 8 分以上（按照 NPS 评估机制执行）	被评估方近三年内完成全国性金融机构省级分支行（或相当等级机构）服务外包项目 21 个。近三年客户平均满意度 NPS 8.5 分	近三年客户服务项目清单、近三年客户满意度调查 NPS	已满足 4 级要求	4 级	XX X	4 级
D5/P 3	网络安全和数据安全能力	原则性	4 级要求-承包方制定并落实了知识产权管理制度、方法和流程，并为之提供了必要的资源投入，以确保所提供的外包服务无知识产权侵权行为或产权纠纷。承包方应确保外包服务活动遵循有关法律、法规和标准，确保不损害发包方及监管机构和主管部门的监管效能。承包方应具有完善的网络安全和数据安全管理体系，并通过行业认可的网络安全和数据安全管理资质认证。按照 GB/T 22080-2016 及后续国家标准的要求对网络安全和数据安全管理进行年度评估，并利用评估结果持续改进网络安全和数据安全管理体系	被评估方制定并落实了知识产权管理制度、方法和流程，所提供的外包服务活动遵循有关法律、法规和标准，具有完善的网络安全和数据安全管理体系，按照 GB/T 22080-2016 及后续国家标准的要求对网络安全和数据安全管理进行年度评估，并利用评估结果持续改进网络和网络安全管理体系	《XXX 知识产权管理制度》、近三年法律违规及相关诉讼情况、《XXX 网络安全和数据安全管理资质认证证书》、《XXX 网络安全和数据安全管理资质证书》	已满足 3 级要求，因未通过行业认可的网络安全和数据安全管理相关资质认证，未满足 4 级要求	3 级	XX X	3 级
D5/P 4	系统支持	非原则性	5 级要求-在主营业务上，普及了具有匹配交付服务的线上系统管理工具，从合规和效率上提升交付质量、服务效率和满意度，系统可提供数据给决策层优化服务、改进企业管理	被评估方在主营业务上，普及了具有匹配交付服务的线上系统管理工具禅道，借助系统相关数据报表，为决策层优化服务、改进企业管理提供数据基础	禅道系统使用情况、案例、相关报表等	已满足 5 级要求	5 级	XX X	5 级

表 D2：承包方能力成熟度评估示例（第 5 页/共 6 页）

能力项编号	能力项名称	能力项类型	评估参考标准	评估记录	评估证据清单	评估结果 (根据具体评估内容记录评估所依据的事实及存在差距等)	预评估等级	评估人	成熟度等级 审议结果
D6/P 1	企业规模	非原创性	4 级要求-供职员工规模，以社保缴存记录为准 咨询规划类：100 开发测试类：500 运行维护类：250 安全服务类：100 业务支持类：250	被评估方申请类别为开发测试类，供职员工共计 700+，均有社保缴纳记录	在职工清单，员工社保缴纳记录	已满足 4 级要求	4 级	XX X	4 级
D6/P 2	财务状况	非原创性	4 级要求-注册资本和实缴资本不少于 2000 万，注册成立时间应不少于 3 年，承包方三年内主营业务没有出现亏损，同时利润率和利润同比保持稳定或上升。前一自然年营业收入达到 1.5 亿，且单一客户收入小于 40%，且所申请类别的收入占比不小于 30% 5 级要求-注册资本和实缴资本不少于 5000 万，注册成立时间应不少于 5 年，承包方三年内主营业务没有出现亏损，同时利润率和利润同比保持稳定或上升。前一自然年营业收入达到 3 亿元，且单一客户收入小于 30%，且所申请类别的收入占比不小于 20%	被评估方注册资本 5900 万，成立 11 年，三年内主营业务没有出现亏损，同时利润率和利润同比保持稳定或上升。迁移自然年营收达 1.5 亿，其单一客户收入小于 40%，所申请类别收入占比 80%	近三年财报、营业执照、上一自然年公司客户收入清单	已满足 4 级要求，因前一自然年营收未达 3 亿，未满足 5 级要求	4 级	XX X	4 级
D6/P 3	经营方向	非原创性	5 级要求-企业主营业务，在市场上具备以下任一特征： 1、高精尖领域，市场潜力大 2、技术含量中等，但市场需求量很大 3、技术含量较低但竞争力强，市场需求巨大	被评估方专注数据库和数据智能，属于核心赛道，技术含量高，市场需求量大	近三年客户清单、合同记录	已满足 5 级要求	5 级	XX X	5 级
D6/P 4	市场份额	非原创性	4 级要求-所申请类别的服务中的全国性金融机构地市级分支行（或相当等级金融机构）客户数量，大于等于 8 家（以商务合同为准）	被评估方所申请类别的服务中的全国性金融机构地市级分支行（或相当等级金融机构）客户数量达到 10 家	近三年客户清单、合同记录	已满足 4 级要求	4 级	XX X	4 级

表 D2：承包方能力成熟度评估示例（第 6 页/共 6 页）

定级结果					
申报定级级别	3 级		评估时间	2022/4/6	
被评估单位	XXX 机构		审议时间	2022/4/7	
定级结论	经评估，XXX 机构满足 3 级别相关要求，金融信息科技外包风险管理能力成熟度级别（承包方）达到 3 级。				
审议小组			签字		日期
<p>备注：评估等级分别为 1-5 级。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（评估更高级别要求时，应将所有更低级别要求作为前置条件），并标明每个能力项的符合性状态。符合性状态应可为符合、不符合、待定。</p> <p>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；</p> <p>b) 如果存在不符合项小于或等于两项，且不为原则项，则评估对象通过该级别评定；否则，则评估对象不通过该级别评定；</p> <p>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。</p>					

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 33136-2016 信息技术服务 数据中心服务能力成熟度模型
 - [3] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
 - [4] GB/T 28448-2019 信息安全技术—网络安全等级保护测评要求
 - [5] T/CCUA-003-2019 金融信息科技服务外包风险管理能力成熟度评估规范
 - [6] T/CCUA-012-2021 金融机构业务连续性管理能力模型与评估
 - [7] 《商业银行数据中心监管指引》（银监办发〔2010〕114号）
 - [8] 《中资商业银行专营机构监管指引》（银监发〔2012〕59号）
 - [9] 《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）
 - [10] 《银行保险机构信息科技外包风险监管办法》（银保监办发〔2021〕141号）
 - [11] ISO 22301-2019 Security and resilience – Business continuity management systems – requirements
 - [12] 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)
-