数据安全能力成熟度服务认证规则

中镡核信（上海）认证服务有限公司

版本号：V2.5　　修订发布日期：2026 年 10 月 21 日，实施日期：2026 年 10 月 23 日

修订页

本实施规则由中镡核信（上海）认证服务有限公司（以下简称“中镡核信”）制定并发布，任何组织及个人未经中镡核信许可，不得以任何形式全部或部分转载、使用。本规则的最终解释权归中镡核信所有。

本规则持续修订，请在中镡核信官网 www.zxhx.org.cn 获取最新版本。

序号	修订内容说明	版本号	日期
1	新建	V1.0	2023 年 6 月 1 日
2	增加了该文件的文件编号，调整了页眉页脚的格式，统一了各章节的章节编号，调整了全文的字体大小和段落设置； 对标 GB／T 37988-2019《信息安全技术 数据安全能力成熟度模型》强调了 4 个安全能力维度和 7 个数据安全过程维度； 明确了认证等级的具体内容。	V2.0	2024 年 10 月 25 日
3	变更了认证证书和认证标志的样式。增加了认证证书和认证标志的图片标识； 对认证证书中的内容进行了调整优化，修改了认证证书名称，新增了认证证书副本样式。	V2.1	2025 年 7 月 16 日
4	依据《国家认监委关于加强认证规则管理的公告》调整了规则结构； 调整了适用范围，具体到业务开展的具体活动； 调整服务认证模式及其组合，具体到具体场景的具体认证模式及其组合。	V2.2	2025 年 8 月 29 日
5	修改了认证证书名称，明确了认证证书状态管理规定； 增加了附件数据安全能力成熟度技术规范，优化了现场审查人日数。	V2.3	2026 年 1 月 21 日
6	依据《国家认监委关于规范服务认证的指导意见》优化了规则结构； 调整初次认证、再认证、监督审查的认证模式和审查方法； 优化了认证证书内容。	V2.4	2026 年 5 月 20 日
7	将受控状态由“非受控”改为“受控”；新增 6.3 审查人日数安排；6.5 文件审查方式调整；新增 5.2 抽样方案；证书模板新增英文翻译样式；依据《国家认监委关于规范服务认证的指导意见》（国认监发〔2026〕3 号）（四）6 将认证级别划分为三级；其余章节编号依次调整。	V2.5	2026 年 10 月 21 日

目录

引言 1
1 适用范围 1
2 认证依据 1
3 引用文件 1
4 认证模式及领域划分 2
4.1 认证模式 2
4.2 认证领域 2
5 认证申请与申请评审 3
5.1 申请范围界定 3
5.2 抽样方案 3
5.3 申请时需提供的文件材料 4
5.4 申请评审 5
6 认证评价 5
6.1 服务特性测评与服务管理审核总体要求 5
6.2 认证审查要求 6
6.3 审查人日数安排 8
6.4 制定审查方案 11
6.5 文件审查 11
6.6 现场审查 12
6.7 审查结论 13
6.8 认证复核与认证决定 14
6.9 认证证书的制作和发放 14
7 获证后监督 14
7.1 监督审查的频次 14
7.4 监督审查决定 15

8 再认证 15
9 认证证书和认证标志 16
9.1 认证证书 16
9.2 认证标志管理要求 16
9.3 认证证书及认证标志样式 18
10 认证证书状态管理规定 19
10.1 证书的保持 19
10.2 证书的变更 21
10.3 证书的暂停、暂停恢复、撤销和注销 21
10.4.认证证书的使用 22
11 收费 22
12 申诉、投诉、争议及处理 22
13 信息报送与公开 22
13.1 信息报送 22
13.2 信息公开 22

引言

为规范数据安全认证的数据安全能力成熟度认证工作，符合国家认证认可监督管理委员会规定的有关要求，保障认证工作的质量及符合性，特制定本规则。针对企业制定切实可行的数据安全能力提升路径，从组织建设、制度流程、技术工具、人员能力等维度全方位提升数据安全能力。

1 适用范围

本规则适用于中镡核信（上海）认证服务有限公司（以下简称“本机构”）基于申请认证组织业务相关的数据处理活动开展的数据安全能力成熟度服务认证。本认证服务类别为服务认证，行业领域 SC12：电信服务；信息检索和提供服务。

2 认证依据

1．GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》（现行有效）。

3 引用文件

1．ZXHX-C9.4-01《数据安全能力成熟度服务认证技术规范》；
2．ZXHX-B9.7《认证证书、标志管理及认证资格处理程序》；
3．ZXHX-B9.13《申诉、投诉与争议处理程序》；
4．ZXHX-C6.2-03《公正性承诺》；
5．ZXHX-C9.3-03《收费管理办法》；
6．ZXHX-C9.7《认证证书和认证标志管理办法》；
7．ZXHX-D9.7-01《保持使用认证证书和认证标志的通知》。

4 认证模式及领域划分

4.1 认证模式

此项服务认证模式为：服务特性测评+服务管理审核+获证后监督。

选用以下服务认证模式:

1) 公开的服务特性检验，简称模式 A；

2) 服务能力确认或验证，简称模式 G；

3) 服务管理审核，简称模式 I。

服务特性测评选用的认证模式为 A+G，服务管理审核适用认证模式 I。

选用的服务认证模式及其组合

基于 GB/T 27207-2020《合格评定 服务认证模式选择与应用导则》可选的服务认证的模式	认证周期	选择与使用的服务认证模式及其组合
(1)公开的服务特性的检验（模式 A）； (2)神秘顾客的服务特性的检验（模式 B）； (3)公开的服务特性的检测（模式 C）； (4)神秘顾客的服务特性的检测（模式 D）； (5)顾客调查（模式 E）； (6)既往服务足迹检测（模式 F）； (7)服务能力的确定和验证（模式 G）； (8)服务设计审查（模式 H）； (9)服务管理审核（模式 I）。	初次认证	服务特性测评选用的认证模式为 A+G，服务管理审核适用认证模式 I。
	再认证	同初次认证
	监督审查	服务特性测评选用的认证模式为 A+G，服务管理审核适用认证模式 I。

4.2 认证领域

服务认证：SC12 电信服务；信息检索和提供服务。

5 认证申请与申请评审

5.1 认证范围界定

认证范围应由认证申请组织提出，认证机构根据认证申请组织的业务类型、所涉及的信息系统及数据处理活动予以界定。认证范围应涵盖以下三个维度：

1) 场所：认证申请组织实际对业务过程或系统进行数据处理活动所在的物理场所。

2) 活动：认证申请组织申请的业务过程或系统的数据安全相关活动。

3) 等级：认证申请组织申请的业务过程或系统的数据处理活动，依据 GB/T •37988-2019 评定的数据安全能力成熟度等级，对应本机构服务认证等级，具体对应关系如下：

等级名称	对应数据安全能力成熟度等级	等级含义
基础级	1 级、2 级	已建立基本的数据安全过程，服务过程可按计划执行，但尚未形成体系化
稳健级	3 级	数据安全过程在组织层面实现规范化执行，服务特性稳定可控
优化级	4 级、5 级	建立量化目标并可度量，能够依据整体目标持续改进和优化服务过程

注：GB/T 37988-2019 规定的 1～5 级成熟度等级，是本机构实施服务特性测评与服务管理审核时使用的评价尺度。

5.2 抽样方案

5.2.1 服务场所抽样

制定抽样方案前，应先对认证申请组织的全部数据服务场所进行分类。场所分类按以下维度进行：

1）按场所规模分类：大型场所（从业人员>500 人、中型场所（从业人员 100~500 人）、小型场所（从业人员≤100 人）。

2）按数据安全风险等级分类：高风险场所（涉及核心重要数据，或敏感个人信息处理量≥10 万条，或一般个人信息处理量≥1000 万条）、中风险场所（涉及一般数据处理，含少量个人信息处理（敏感个人信息处理量低于 10 万条，或一般个人信息处理量低于 1000 万条））、低风险场所（无个人信息处理或仅涉及公开数据）。

应要求认证申请组织提供场所清单，清单中应包含每个场所的名称、地址、功能定位、人员规模、数据处理量级及风险等级等信息。

当同一法人的认证申请组织存在一个以上场所提供同一类型服务时，按以下规则进行抽样：

1）本次审查涉及的场所≤3 个，全量抽样；

2）本次审查涉及的场所＞3 个，按照 $n\sqrt{X}$ 进行抽样，其中 X 为场所总数量，n 为抽样系数（初次认证抽样系数范围：1.8-2，监督认证抽样系数范围：1.1-1.2），即抽样场所数为 $n\sqrt{X}$ 个，结果不为整数时向上取整。

注：当计算出的抽样场所数超过可抽样场所总数时，应对全部可抽样场所进行评价；抽样系数 n 根据所申请的数据安全能力成熟度等级选取。

5.2.2 过程域（PA）抽样

初次认证和再认证审查对所有 PA 采取全量评价，不涉及抽样。

监督审查采用 PA 抽样审查方式，不要求对全部 PA 进行全量评价，但两次监督审查应覆盖全部 30 个 PA。具体规则如下：

1）抽样 PA：对全部 PA 进行抽样评价，抽样比例应不低于 PA 总数的 50%。

2）覆盖要求：两次监督审查的 PA 评价范围应均衡覆盖数据全生命周期过程域与通用安全过程域两个维度。

3）场所抽样：监督审查的场所抽样规则按照 6.2.1 执行，但可结合上次审查结果和风险评估适当调整抽样范围。

5.3 申请时需提供的文件材料

申请认证应提交认证申请书，并随附以下文件：

1) 有效法律地位证明复印件及适用时从事相关服务的资质和任何行政许可证明复印件；

2) 国家企业信用信息公示系统年度报告电子版；

3) 数据安全能力成熟度自评估表；

4) 已获数据安全能力成熟度评估证书复印件及最近一次评估报告复印件（适用时）；

5) 其他认证所需相关材料。

5.4 申请评审

认证机构根据认证依据、程序等要求，对申请方提交的申请资料进行评审，确认资料的完整性、准确性和符合性。并将评审结果（包括受理、退回修改、不受理）告知认证申请组织，并保存评审记录。

存在以下任一情形的，不予受理:

(1) 近一年内存在严重行政处罚；

(2) 列入国家信用信息严重失信主体相关名录:

(3) 其他情形。

若决定受理该申请，本机构将通知认证申请组织并签订认证合同。

6 认证评价

6.1 服务特性测评与服务管理审核总体要求

认证机构对申请组织的数据安全能力成熟度等级开展服务特性测评和服务管理审核，主要依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》的内容进行。

认证评价是对数据安全过程包括数据生存周期安全过程和通用过程，并对组织建设、制度流程、技术工具及人员能力 4 个安全能力维度进行审查评价。

GB/T37988-2019《信息安全技术数据安全能力成熟度模型》中，“技术工具”部分是服务特性测评的要求；“组织建设”、“制度流程”、“人员能力”部分是服务管理审核的要求。

6.2 认证审查要求

6.2.1 审查内容与基本要求

1) 审查内容

(1) 服务管理审核

审查内容覆盖数据安全处理活动服务认证的“组织建设”、“制度流程"、" 人员能力 ", 适用于各类数据安全组织数据安全全生命周期和通用安全的管理能力核查及认证过程中的服务管理的审查。

(2) 服务特性测评

审查内容覆盖数据安全处理活动服务认证的 “技术工具”，适用于各类数据安全组织数据安全全生命周期和通用安全能力核查及认证过程中的技术能力的审查。

2) 审查及人员的基本要求

审查需遵循客观公正、全程留痕原则，审查过程应形成完整的核查记录等资料，确保审查结果可追溯、可复核。认证机构应当充分考虑审查所涉及的人员能力、专业能力和公正性要求，确定审查组成员，应当根据申请组织覆盖的活动的专业技术领域选择具备相关能力的审查员组成审查组，必要时可以选择技术专家参加审查组。审查组中的审查员承担审查任务和责任，审查前应完成对组织行业特点、组织建设、制度流程、技术工具和人员能力及业务系统的前期调研。

3) 审查方法

人员访谈：通过与被评估方相关人员进行交流、讨论、询问等活动，对数据的处理、保障措施设计和实施情况进行了解、分析和取证，以评估数据安全保障措施有效性。数据处理者需要安排熟悉数据流转过程，以及承载数据的应用、系统、网络情况的人员参加访谈；

文件审查：查阅数据安全相关文件资料，如组织数据安全管理活动制度、业务技术资料和其他相关文件，用以评估数据安全管理活动相关制度文件是否符合标准要求的一种方法。通常在评估准备阶段以及数据安全管理活动类基线评估部分使用该方法，组织需要事先完整准备上述文档以供查阅；

配置检查：检查范围涵盖数据处理系统、网络设备、安全设备等的配置。例如，检查数据库管理系统的用户权限配置是否符合最小化授权原则，网络设备的访问控制列表（ACL）是否正确设置以限制对敏感数据的访问，防火墙的规则配置是否能有效防止外部攻击等。实施方式：可以通过登录设备管理界面查看配置参数，或使用专业的配置管理工具导出配置文件进行分析。同时，对照相关标准和最佳实践，检查配置是否存在安全漏洞或不符合规范的地方。

旁站式验证：申请组织相关人员演示、审查员查看承载数据的应用、系统、网络，包括数据采集界面、数据展示界面、数据存储界面、数据操作日志记录等，以评估数据安全保障措施是否有效的一种方法，通常在评估过程中深入组织现场调研时使用，组织需要安排相关人员进行现场演示，评估人员根据系统演示情况进行查验，如系统存在高度保密性、可用性的要求，评估可通过事后提供日志列表或测试环境等方式进行；

工具测试：采用适配工具或技术手段测试数据载体，分析输出结果以验证数据安全保障措施的有效性。数据处理者需提前搭建测试环境，保障工具接入运行。检测前需预判对数据载体及业务的影响；对业务不可中断的核心系统与应用，优先采用模拟系统、离线环境等非侵入式验证方式。

4) 评价准则

基于认证机构《数据安全能力成熟度服务认证技术规范》的要求进行评价。

6.3 审查人日数安排

6.3.1 基本原则

1. 电信服务；信息检索和提供服务领域的现场审查至少包括服务特性要求测评和服务管理要求审核，现场审查人日数不得低于 3 人日。服务特性要求测评的人日数不宜低于服务管理要求审核的人日数，且应当与其工作量相匹配。

2. 在标准计算得出的人日基础上，可结合组织规模、业务复杂程度度上限为±20%。

组织规模系数见下表：

组织规模划分	规模系数	说明
小型（员工 ≤ 100 人）	1.0	组织架构简单，文件层级少、覆盖范围窄
中型（员工 100～500 人）	1.1	多部门协同，文件体系分支较多，核查工作量提升
大型（员工 ＞ 500 人）	1.2	多层级分支机构、多业务线，文件数量庞大、审批链条复杂

业务复杂程度上浮比例见下表：

复杂等级	上浮比例	判定标准
低	+0%	满足以下任意条件： 支撑业务系统≤3 套；无外部机构数据交互；服务地域限于单一区域
中	+10%	满足以下任意条件： 支撑业务系统 4～10 套；存在少量外部接口数据交互；服务地域覆盖 2～3 个区域
高	+30%	满足以下任意条件： 支撑业务系统≥11 套；存在多外部机构间数据交互或跨境数据流通；服务地域覆盖全国或多省

数据安全风险等级上浮比例见下表：

风险等级	上浮比例	判定标准
低	+0%	无个人信息处理或仅涉及公开数据
中	+10%	涉及一般数据处理，含少量个人信息处理（敏感个人信息处理量低于 10 万条，或一般个人信息处理量低于 1000 万条）
高	+30%	涉及核心重要数据

1. 总审查人日 = 文件审查人日 + 现场审查人日，全部审查人日核算不含审查组往返交通、差旅等候时间。

2. 最小计量单位为 0.5 人日（4 小时）。

3. 所有计算结果统一以 0.5 人日为最小计量单位，结果向上进位取整。

6.3.2 文件审查人日计算

文件审查人日以申请数据安全能力成熟度各等级对应的文件审查基准人日为基准数值，乘以组织规模系数得出具体审查人日数，最终以 0.5 人日为最小计量单位，结果向上进位取整。上述计算结果为最低参考人日，审查组长可根据受评价组织的实际情况适当增加。

申请等级	对应数据安全能力成熟度等级	文件审查基准人日	基准工作小时	说明
基础级	1 级	1.0	8	组织数据安全工作仅依托临时需求、个人经验零散开展，无稳定标准化机制；文件审查重点核查基础合规文档是否存在，整体配套安全文档数量少、不成体系，仅验证基础资料完整性。
	2 级	1.0	8	组织在业务系统层面实现安全过程规划、执行、验证、跟踪闭环管理；文件审查需核查安全过程规划文件、全流程配置管理文件、执行验证记录、偏差跟踪修正记录，配套执行与跟踪类记录文件体量明显增加。
稳健级	3 级	1.0	8	组织层面完成标准化数据安全过程制度建设，具备可重复落地的标准化流程、跨业务系统及外部协同安全实践机制；文件审查核查完整标准化流程文档、跨域安全协调机制文件、过程执行结果与全量留存记录。
优化级	4 级	1.5	12	组织建立可度量的数据安全目标，依托量化指标管控全流程、以量化数据驱动整改行动；文件审查重点核查安全指标台账、过程量化测量报表、数据分析及量化管控相关支撑文件。
	5 级	2.0	16	组织建立全域规程对比、常态化缺陷消除与迭代改进机制，围绕整体业务目标持续优化数据安全能力；文件审查覆盖组织级改进机制文件、流程迭代复盘材料、行业对标分析及最佳实践落地配套材料。

文件审查人日计算公式如下：

文件审查人日 = 文件审查基准人日 × 组织规模系数

计算结果统一以 0.5 人日为最小计量单位，结果向上进位取整。

6.3.3 现场审查人日计算

现场审查人日通过综合数据安全能力成熟度各等级对应的现场审查基准人日、组织规模、业务复杂度、数据风险等级这四项维度去核算，最小计量单位为 0.5 人日，结果向上进位取整。

申请等级	对应数据安全能力成熟度等级	现场审查基准人日	基准工作小时	说明
基础级	1 级	3.0	16	组织数据安全工作仅依靠临时需求、个人经验零散落地，无标准化稳定执行机制；现场审查以核验一线实操场景基础合规底线，确认基础安全动作落地情况为主。
	2 级	4.0	32	组织在业务系统层面建立安全规划、执行、验证、跟踪闭环流程；现场核查比对现场实操、规划文件、执行记录与跟踪管控措施，验证全流程执行一致性与实际管控效果
稳健级	3 级	5.0	40	组织已建立标准化、可复用的数据安全全过程制度与跨业务协同机制；现场全业务场景核验标准化流程落地情况，核查跨部门、跨系统安全实践协同执行效果。
优化级	4 级	6.0	48	量化控制级：组织建立可度量的数据安全目标，依托量化指标管控安全全过程；现场核查量化指标采集流程、数据分析应用、阈值预警与量化整改管控措施落地实效等。
	5 级	10.0	80	组织建立全域流程迭代、缺陷整改、对标改进常态化机制；现场全维度核验高阶安全管控落地、全流程持续改进机制运行、行业对标成果应用，以及安全实践与组织整体目标协同优化成效。

判定标准逻辑关系说明：

同一等级（低/中/高）中各判定条件为"和"（AND）关系，须同时满足方可归入该等级；当各维度落入不同等级时，按"就高原则"（取最大等级）确定最终等级。

现场审查人日计算公式如下：

现场审查人日 = 现场审查基准人日 × 组织规模系数 ×（1 + 业务复杂上浮比例 + 风险等级上浮比例）

计算结果统一以 0.5 人日为最小计量单位，结果向上进位取整。

6.3.4 监督审查人日计算

监督审查仅开展现场审查工作，不执行全套完整文件审查，必要时可对关键文件变更情况进行简要核查。监督审查人日基数为初次认证现场审查核算人日的 1/2。

监督审查人日计算公式如下：

监督审查人日 = 初次认证现场审查核算人日 ÷ 2

计算结果统一以 0.5 人日为最小计量单位，结果向上进位取整，最低不得低于 1.0 人日（8 小时）。

6.3.5 特殊情形

特殊业务情形	核算处理规则
多场所运营组织	以组织总部的统一管理审查为基础，结合各场所业务实际安排抽样：业务相似、风险相近的场所可按审查类型和场所总数合理确定抽样数量；业务差异大或风险显著不同的场所应扩大抽样比例或逐一审查。审查总人日按总部及被抽样场所的实际工作量综合核算，不按场所数量简单累加。

6.4 制定审查方案

认证机构根据确定的认证申请组织的认证范围，依据标准和认证模式等情况，按照认证机构的认证程序，编制审查方案，开展认证活动。

6.5 文件审查

审查组原则上采用非现场形式，通过对受审查组织提交的数据安全服务认证的申请书、数据安全能力成熟度自评估表、服务特性检验报告（适用时）以及相关佐证材料进行文件审查，对组织的数据安全管理制度、流程、记录等文件进行全面检查，验证其完整性和符合性。审查组需确保文件内容覆盖服务认证业务开展的各个方面，并与组织的实际业务活动相匹配。对文件审查中发现的不符合项，申请组织应及时修改、补充提交必要的文件，文件整改实施期限原则上不超过 10 个工作日。

审查组出具文件审查报告，给出是否进行现场评价的建议及现场评价中需重点关注的事项。

文件审查人日数根据申请级别不同为 1-3 人日。

6.6 现场审查

6.6.1 总体要求

现场审查需进行服务特性测评和服务管理审核。

审查组须在申请方的现场进行公开的服务特性检验和服务能力确认或验证,审查内容为GB/T37988-2019《信息安全技术数据安全能力成熟度模型》中的技术工具部分。

审查组须在申请方的现场开展服务管理审核，审查内容为 GB/T37988-2019《信息安全技术数据安全能力成熟度模型》的组织建设、制度流程、人员能力部分。

现场审查人日数根据受审查组织的规模大小，审查现场场地分布，服务活动复杂程度来确定，一般为 3-20 人日。

6.6.2 首次会议

现场审查开始后，召开首次会议，申请组织的管理层和涉及到被审查部门的负责人员应参加会议。参会人员均应签到，审查组保留首次会议签到表和会议记录。首次会议至少包含以下内容：

(1) 介绍审查组成员及其职责；

(2) 阐明审查的目的和准则；

(3) 确定审查日程安排；

(4) 介绍审查方法和程序；

(5) 确认审查组陪同人员、所需资源和设施；

(6) 说明审查结果的提交方法和可能存在的审查结论。

6.6.3 审查实施

对受审查方的组织架构、人员能力、制度流程、技术工具等进行调研，根据有关过程域进行分析，获取初步分析结果，支撑后续综合评定工作，包括以下工作内容：

(1) 过程域解析，选取过程域 PA：针对受审查方的数据相关的业务现状，选取适当的数据安全过程域 PA，对不适用于组织的数据安全过程域 PA 或基本实践 BP 进行裁减；

(2) 执行基本实践 BP：依据标准和受审查方所申请等级的数据安全 BP 要求，从组织建设、制度流程、技术工具和人员能力等维度进行解析，输出后续阶段的评价依据；

(3) 过程域分析，基于选择的过程域 PA 范畴，针对各项过程域 PA 对组织的数据安全运

行情况进行初步分析，确定综合评价的方式。

基于机构内部《数据安全能力成熟度服务认证技术规范》的要求，确定申请组织整体的数据安全能力成熟度等级。

6.6.4 末次会议

现场审查结束前，审查组应与申请组织负责人进行会晤，表明审查组现场评价的意见。审查组同申请组织召开末次会议，申请组织的管理层和涉及到被审查部门的负责人员应参加会议。参会人员均应签到，审查组保留末次会议签到表和会议记录，末次会议至少包含以下内容：

(1) 告知现场审查结论：推荐注册/不推荐注册/待纠正措施实施并验证确认符合要求后推荐注册；

(2) 告知审查后续事项和发证流程；

(3) 告知如何获得证书后，到期换证、变更及年度监督审查的要求；

(4) 告知投诉、申诉程序。

如审查组长在本阶段审查中列出不符合项，则需在该阶段末次会议中由申请组织现场签字确认，并要求申请组织在整改期限之内按照要求完成不符合项的纠正/纠正措施，并由审查组进行验证。审查组成员需及时向审查组长报告整改情况，由审查组长安排后续事宜。

6.6.5 不符合项的纠正/纠正措施的验证

本机构针对末次会议提出的不符合项，验证申请组织所采取的纠正/纠正措施及其结果的有效性。

6.7 审查结论

审查组对现场审查中收集的所有信息和证据进行汇总分析，评价审查发现并就审查结论达成一致。审查组长根据审查组的审查结果与内部讨论意见，负责编制审查报告。审查报告编制完成后，由认证机构内部专家组进行评审。评审通过后，由认证机构的认证决定或复核人员对审查报告进行复核与批准，确保审查报告的权威性与有效性。

6.8 认证复核与认证决定

(1) 认证决定或复核人员依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》的要求，对申请评审、评价过程和结论等进行复核的基础上，给出认证决定意见：

- 达到申请组织申请的数据安全能力成熟度等级，批准认证决定；
- 未达到申请组织申请的数据安全能力成熟度等级，不批准认证决定。

(2) 认证决定或复核人员为本机构人员，审查组成员不得参与对审查项目的认证决定；

(3) 对于不符合认证要求的申请组织，本机构以书面的形式明示其不能获得认证的原因；

(4) 申请组织如对认证决定结果有异议，可在 10 个工作日内向本机构提出申诉，本机构进行申诉受理，并将处理结果通知申诉方。

6.9 认证证书的制作和发放

认证机构对于评价结果符合申请认证标准要求的，本机构将向申请组织提供书面审查报告并同时颁发服务认证证书。

7 获证后监督

7.1 监督审查的频次

认证机构在认证证书有效期内，通过认证评价对获得认证的专业机构进行持续监督，年度监督审查至少每个日历年进行一次，初次认证后的第一次监督审查在认证证书颁证之日起 12 个月内进行。若发生下述情况可适当增加监督频次：

1) 获证组织的服务活动出现严重质量问题，如：发生数据安全事故或在数据安全方面有重大投诉，并经查实为获证组织责任时；

2) 认证机构有足够理由对获证组织服务与认证要求的符合性提出质疑时；

3) 有足够信息表明获证组织因变更组织机构、服务场所、环境条件等，可能影响服务符合性或一致性时；

4) 违反法律法规、国家行业监督及媒体曝光等重大问题的情况；

5) 发生其他影响符合认证要求的能力变化的特殊情况时。

若超过期限未能实施监督审查的，应按照《认证证书、标志管理及认证资格处理程序》的要求进行管理；

7.2 监督审查的方式和内容

监督审查的一般采取现场审查为主、远程审查为辅的方式，内容包括服务特性测试评和服务管理审核。监督至少应包括服务管理审核，且在一个认证周期内至少开展一次服务特性检验，监督采用条款抽样的方式开展，抽样 PA 的数量应不低于认证依据条款的 1/2。

每次监督审查应包括对以下方面的审查：

(1)初次认证不符合项对应过程域的纠正措施及效果；

(2)内部审查和管理评审；

(3)为持续改进而策划的活动的进展；

(4)持续的运作控制及留痕；

(5)投诉的处理；

(6)获证组织任何变更；

(7)标志的使用和(或)任何其他对认证资格的引用；

(8)上次审查后发生的数据安全事件的调查与处理。

7.3 监督审查的时间

监督审查的时间应根据获证组织规模、认证范围、成熟度等级确定，一般不少于初次认证审查时间的 1/2。

7.4 监督审查决定

监督审查完成后，本机构根据监督审查情况和审查报告，做出保持、暂停或者撤销认证证书的决定。涉及证书状态变化的，需向证书持有者发出暂停、撤销和恢复暂停认证证书和认证标志的通知书。对于被撤销认证证书资格的组织，应于接到通知书的 5 个工作日内将证书交还至本机构。本机构将在官方网站上公布年度监督审查结果。

8 再认证

认证证书有效期三年,若获证组织申请继续持有认证证书，应在证书有效期满前三个月向

本机构提出再认证申请,并提交相关资料。

再认证的流程和过程、需审查的内容与初次认证相同，再认证的认证决定通过后，为获证组织换发新的认证证书。

9 认证证书和认证标志

9.1 认证证书

本机构的服务认证证书依据在国家认监委 (CNCA) 备案的证书要求进行统一制作、发放。未经本机构认证授权，其他组织或个人不得自行翻印或仿制。认证证书英文样式仅为翻译文件，翻译文件不具有法律效力、不得单独使用。

认证证书的内容包括:

1) 获证组织名称、地址和统一社会信用代码（或组织机构代码），该信息应与其法律地位证明文件的信息一致；

2) 获准认证的场所范围、系统名称或业务名称。若认证覆盖多场所，应包含覆盖的相关场所的名称和地址信息；

3) 认证依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》；

4) 证书编号；

5) 认证机构名称；

6) 有效期的起止年月日；

7) 证书应注明：“获证组织必须定期接受监督审查并经审查合格此证书方继续有效”的提示信息；

8) 证书查询方式。在本机构网站（zxhx.org.cn）上查询认证证书有效性，以便于社会监督。

9.2 认证标志管理要求

本机构按照《认证证书和认证标志管理办法》，明确认证标志使用者的权利和义务，对获得认证的组织使用认证标志的情况实施有效跟踪调查，发现其认证的服务不能符合认证要

求的，将及时作出暂停或者停止其使用认证标志的决定，并予以公布。

获得数据安全能力成熟度（DSMM）认证的组织应当在广告等有关宣传中正确使用认证标志，可以将数据安全能力成熟度（DSMM）认证标志悬挂在获得服务认证的区域内，但不得利用数据安全能力成熟度（DSMM）认证标志误导公众认为其产品、管理体系通过认证。

ZXHX

9.3 认证证书及认证标志样式



数据安全能力成熟度服务认证证书

证书注册号:CNCA-R-2023-1341-yyyynnn

兹 证 明

XX公司

统一社会信用代码:xxxxxxxxxxxxxxxxx

注册地址:xxxxxxxxxxxxxxxxx

评估符合

GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》

数据安全能力成熟度X级要求

服务认证等级达到

XX级

认证规则

ZXHX-RZGZ-DS-202601《数据安全能力成熟度服务认证规则》

经营地址:xxxxxxxxxxxxxxxxx

认证范围:xxxxxxxxxxxxxxxxxx

颁证日期:xxxx年x月xx日　　有效期至:xxxx年x月xx日

获证组织必须定期接受监督审查并经审查合格此证书方继续有效

本证书信息可在中镡核信（上海）认证服务有限公司官方网站（www.zxhx.org.cn）上查询

证书信息

扫描二维码验证本证书有效性

中镡核信(上海)认证服务有限公司 证书专用章

王艳

签发人

中镡核信(上海)认证服务有限公司

地址:上海市静安区泰州路415号305室

图 1：认证证书样式



图 2：认证标志样式

10 认证证书状态管理规定

本机构参照《认证证书和认证标志管理办法》对认证证书状态进行管理。机构依据认证基本规范与规则，为达到数据安全能力成熟度模型相应等级的申请组织，在认证决定通过后的 30 日内出具含组织名称、地址、认证范围、认证依据、证书编号、发证机构及有效期等内容的认证证书，获证组织需正确使用认证证书，业务发生重大变化时须申请变更，未变更或不符合要求不得使用，且不得误导公众；机构跟踪调查证书使用情况，对不能符合认证要求的，将暂停其使用直至撤销认证证书，并予以公布；对撤销或注销的证书机构需收回，无法收回的机构会在官网公示。

10.1 证书的保持

10.1.1 认证证书的保持需满足以下条件

(1) 获证组织的法律地位、资质持续符合国家的最新要求，认证范围内的法律地位文件和资质持续有效；

(2) 按认证规则规定的周期和程序接受监督审查并符合要求；

(3) 认证证书和标志的使用符合规定的要求；

(4) 在证书有效期内，获证服务的一致性能够得到保持，且当需要时进行的抽样测评能够证明获证服务仍然符合相应认证标准；

(5) 按规定要求及时向本机构报告相关变更情况；

(6) 按时缴纳规定的认证费用；

(7) 本机构规定的其它需要保持认证证书的条件，如，未发现有其他不符合国家相关法律法规、国家行业监督及媒体曝光等重大问题的情况；

(8) 符合认证规定的其他要求。

认证证书有效期为 3 年，若获证组织提出申请继续持有认证证书，应在证书有效期满前 3 个月向公司提出再认证申请，并重新签订认证合同，开展再认证工作，符合认证要求的换发新证书。

10.1.2 证书有效期内的通报要求

获证组织发生以下情况时，需及时联系本机构，进行信息通报：

a. 发生服务活动方面的事故或在服务活动方面有重大投诉；

b. 提供的服务被质量或市场监管部门认定不合格；

c. 相关情况发生变更，可能影响服务能力符合认证要求，包括：服务交付过程或质量体系方面以及可能影响继续提供获证服务能力的任何组织变更，如法律地位、生产经营状况、组织状况或所有权变更，服务的工作场所变更、联系方式变更，服务覆盖的活动范围变更，服务能力和服务过程的重大变更等；

d. 出现影响服务能力运行的其他重要情况（如认证标准变更或认证范围扩大或缩小等）等。

一般情况下，应在更改/变动后 1 个月内通知本机构，如发生上述 a)、b）条情况时，应在事故或问题发生后 48 小时内通知本机构（特殊情况不超过 1 周）。本机构根据情况决定是否进行调查，涉及变更的按本文件 10.2.1 实施认证变更评价工作，在评价后对符合要求的予以批准变更；或按本文件 10.3 做出认证暂停、撤销的决定。

10.2 证书的变更

10.2.1 影响认证的变更

获证后出现下列情况的变更应向认证机构提交变更申请及相关附件：

(1) 获证组织名称、注册地址发生变更；

(2) 证书覆盖范围发生变更，包括服务覆盖的活动、场所等；

(3) 服务能力和服务过程的重大变更等；

(4) 认证级别发生变更（适用时）；

(5) 认证机构规定的其他应当变更的情形。

本机构将根据申请变更的具体情况按照相关程序决定是否采取文件审查、服务特性测评、服务能力确认或验证、服务管理审核等评价工作，在评价后对符合要求的予以批准变更。

其中，认证级别的提高按初次认证执行。

10.2.2 认证要求的变更

获证组织应始终满足认证要求，当认证要求发生变化时，认证机构将以书面或其他方式将其认证要求的任何变更通知获证组织，并对其是否符合新的要求予以验证。为确保实施这些要求，获证组织可能需要与本机构补充签署或修订认证合同。

10.3 证书的暂停、暂停恢复、撤销和注销

当获证组织不再符合认证要求，认证机构对证书予以暂停直至注销。获证组织在证书有效期内可申请暂停或注销。机构应采用适当方式对外公布相关信息。

暂停期内，获证组织可提出恢复证书的申请，经认证机构评审、批准后，可恢复使用证书。在证书暂停期间，获证组织不得继续使用认证证书和认证标志。通常认证证书暂停的时间为期6个月，超过该时间将自动转化为撤销证书。

认证证书的暂停、恢复、撤销和注销按照《认证证书、标志管理及认证资格处理程序》执行。

10.4.认证证书的使用

认证证书的使用应符合机构的《认证证书和认证标志管理办法》的要求。

11 收费

为加强本机构对申请组织进行数据安全能力成熟度认证的收费管理，规范认证收费行为，保护认证双方的利益，促进数据安全能力成熟度认证业务的发展，特制定了收费管理办法，具体参见《收费管理办法》。

12 申诉、投诉、争议及处理

本机构参照《申诉、投诉与争议处理程序》进行管理。

13 信息报送与公开

13.1 信息报送

认证机构在颁发认证证书后，应当在次月 10 日前按照规定的要求将认证结果相关信息报送国家认证认可监督管理委员会。

13.2 信息公开

认证机构为方便认证企业、广大消费者获得认证信息，发挥社会监督作用，通过网站向社会公布获证企业证书信息。与认证相关的需向社会公众公告的相关信息，主要包括获证企业证书信息、证书暂停、恢复、撤销与注销信息、《数据安全能力成熟度服务认证规则》、《认证证书和认证标志管理办法》、《投诉、申诉和争议的处理程序》、《收费管理办法》和《公正性承诺》。

（以下无正文）