数据安全能力成熟度服务认证规则

ZXHX

中镡核信（上海）认证服务有限公司

版本号：V2.3　　修订发布日期：2026 年 1 月 21 日，实施日期：2026 年 1 月 21 日

目录

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安全管理活动开展的数据安全能力成熟度服务认证。

2 参考文件

1．国家认证认可监督管理委员会 2025 年第 9 号《国家认监委关于加强认证规则管理的公告》；
2．国家认证认可监督管理委员会 2025 年第 16 号《质量管理体系认证规则》；
3．CNAS-CC105：2020《确定管理体系审核时间(QMS、EMS、OHSMS)》；
4．GB/T 27065-2015《合格评定 产品、过程和服务认证机构要求》；
5．GB/T 27207-2020《合格评定 服务认证模式选择与应用导则》。

3 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）；
2．ZXHX-C9.4-01《数据安全能力成熟度服务认证技术规范》。

4 引用体系文件

1．ZXHX-B9.7《认证证书、标志管理及认证资格处理程序》；

2．ZXHX-B9.13《申诉、投诉与争议处理程序》；

3．ZXHX-C6.2-03《公正性承诺》；

4．ZXHX-C9.3-03《收费管理办法》；

5．ZXHX-C9.7《认证证书和认证标志管理办法》；

6．ZXHX-D9.7-01《保持使用认证证书和认证标志的通知》。

5 认证审查人员能力要求

参与认证活动的审查员、技术专家等人员应具备相应的专业知识、技能和经验，熟悉 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》标准及相关法律法规要求，且经过认证机构的培训和考核合格。认证机构应建立认证人员档案，对其工作表现进行记录和评价，确保认证人员的能力和行为符合认证工作的要求。

认证审查人员应当取得国家认证认可监督管理委员会确定的认证人员注册机构颁发的服务认证审查人员注册资格。

认证审查人员应当遵守与从业相关的法律法规，对认证审核活动及相关认证审核记录和认证审核报告的真实性承担相应的法律责任。

6 认证模式及领域划分

6.1 认证模式

基于 GB/T 27207-2020《合格评定 服务认证模式选择与应用导则》可选服务认证的模式包括 A-I：

(1) 公开的服务特性的检验，简称模式 A；

(2) 神秘顾客（暗访）的服务特性的检验，简称模式 B；

(3) 公开的服务特性的检测，简称模式 C；

(4) 神秘顾客（暗访）的服务特性的检测，简称模式 D；

(5) 顾客调查（功能感知），简称模式 E；

(6) 既往服务足迹检测（验证感知），简称模式 F；

(7) 服务能力的确定和验证，简称模式 G；

(8) 服务设计审核，简称模式 H；

(9) 服务管理审核，简称模式 I。

6.1.1 初次服务认证模式及其组合

本机构对于初次服务认证选择的服务认证模式及其组合为：模式 A+模式 I。

6.1.2 再认证和监督认证模式及其组合

本机构再认证和监督认证时，服务认证模式及其组合参照初次服务认证模式及其组合。

6.2 认证领域

服务认证：SC12 电信服务；信息检索和提供服务。

7 抽样

7.1 人员类

抽样基数为组织架构中涉及认证范围的各部门代表，及承担数据安全职责的人员，按“核心角色-业务角色-支持角色”分类统计总数；抽样方法以分层为基础且关键角色必抽，核心角色 100%抽样，其他角色按数据接触敏感度分层随机抽样；抽样量按角色类型与敏感度确定：核心角色全检，业务角色高敏感抽≥30%、中低敏感抽≥20%，支持角色抽≥25%。

7.2 活动场地类

抽样基数依据访谈主体确定，访谈对应主体时，即以该主体涉及认证范围的相关物理场地总数为基数；抽样方法采用定向抽样，精准锁定访谈主体关联的场地；抽样量按定向抽样原则，覆盖访谈主体下所有相关场地。

8 审核方法

审查组按照审核计划安排实施审核，通过人员访谈、文档审查、配置核查、工具测试和旁站式验证等方法进行审核，具体审核方法如下：

人员访谈：评估人员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；

文档审查：文档查验是指评估人员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评估人员查阅；

配置核查：核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：旁站式验证是指组织相关人员演示、评估人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：评估人员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。

9 服务认证单元划分及认证分级

9.1 认证单元划分

数据安全能力成熟度服务认证以组织为单位，以数据为中心，基于数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全和通用安全 7 个数据安全过程维度，围绕组织建设、制度流程、技术工具、人员能力 4 个安全能力维度，划分认证单元。

9.2 认证等级

依据 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等级分为 5 级，具体包括：1 级是非正式执行级，2 级是计划跟踪级，3 级是充分定义级，4 级是量化控制级，5 级是持续优化级。其中 5 级为最高级。

10 服务特性评价要求

DSMM（Data Security Maturity Model）即数据安全能力成熟度模型，其服务特性评价要求是依据《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）和《数据安全能力成熟度服务认证技术规范》，对组织的数据安全能力相关的组织建设、制度流程、技术工具及人员能力等进行评价。

10.1 能力维度

组织建设：评估组织是否设立了专门的数据安全岗位和人员，负责数据安全策略的制定和执行，以及是否有明确的职责分工。

制度流程：考查组织是否建立了完善的数据安全管理制度和流程，包括数据采集、传输、存储、处理、交换、销毁等各个环节的安全规范，以及制度流程的执行情况和更新机制。

技术工具：了解组织是否采用了必要的数据安全技术工具，如数据加密、访问控制、数据脱敏、数据备份恢复等，以及技术工具的功能是否满足数据安全需求，是否与组织的业务

系统相适配。

人员能力：评估组织内人员的数据安全意识和专业能力，包括是否进行了数据安全培训，人员是否具备数据安全相关的知识和技能，能否有效地执行数据安全制度和流程。

10.2 成熟度等级维度

1 级 - 非正式执行级：数据安全能力处于初始阶段，执行过程随机、无序，主要依赖个人经验，没有形成系统化的安全管理体系。

2 级 - 计划跟踪级：在业务系统级别开始主动进行安全过程的计划与执行，能够跟踪和控制执行进展，但尚未形成全面的体系化管理。

3 级 - 充分定义级：在组织级别实现了安全过程的规范执行，将标准过程制度化，过程可重复执行，执行结果可核查。

4 级 - 量化控制级：建立了量化的安全目标，安全过程可度量，能够通过数据统计和分析来评估和改进数据安全能力。

5 级 - 持续优化级：根据组织的整体目标，不断改进和优化组织的数据安全能力和安全过程的有效性，能够快速适应业务和技术的变化。

10.3 数据全生命周期过程

数据采集安全：评估数据采集的合法性、合规性和准确性，是否明确了数据采集的范围和目的，是否获得了必要的授权。

数据传输安全：考查数据在传输过程中的保密性、完整性和可用性，是否采用了加密等技术手段防止数据泄露和篡改。

数据存储安全：关注数据存储的安全性和可靠性，包括存储介质的管理、数据备份与恢复策略、数据加密存储等。

数据处理安全：评估数据处理过程中的安全风险，如数据脱敏、访问控制、数据审计等，确保数据处理的合法性和合规性。

数据交换安全：考查数据在不同组织或系统之间交换时的安全措施，如数据共享的审批流程、数据格式的转换、数据加密等。

数据销毁安全：关注数据销毁的彻底性和合规性，是否有明确的数据销毁流程和记录，

确保数据在不再需要时能够被安全删除。

通用安全：包括安全策略、安全评估、安全培训等通用的数据安全管理内容。

10.4 评价要求

依据《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）要求，结合《数据安全能力成熟度服务认证技术规范》和评价结果，确定数据安全能力成熟度等级（非正式执行、计划跟踪、充分定义、量化控制、持续优化）。

11 认证程序

11.1 认证申请

申请组织提交数据安全能力成熟度（DSMM）认证申请及附件材料。资料包括，但不限于：

(1) 有效的营业执照复印件；

(2) 组织架构图；

(3) 符合 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》的现行有效的数据安全能力成熟度成文文件，至少包含管理策略、管理规定、实施细则等内容；

(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（如有）；

(5) 拟申请的服务认证等级；

(6) 提供企业征信佐证截图；

(7) 其他有关资料。

11.2 认证申请的评审

(1) 对申请材料进行审查，确定其完整性和符合性。对申请组织提交的申请书和申请资料进行内容审查并保存审查记录，以确保：

1) 认证要求明确、形成文件并得到理解；

2) 本机构和申请组织之间在理解上的差异得到解决；

3) 对于申请的认证内容以及后续现场审核场所，本机构有能力开展审核服务。

(2) 若存在被执法监管部门责令停业整顿或在信用中国网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）上被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，本机构不予受理其认证申请；

(3) 通过认证申请评审后，本机构将与申请组织签订认证合同，正式受理该申请；

(4) 若文档审查存在较多问题，需要及时反馈给申请组织待其修改后重新提交，或向申请组织发出不予受理的通知。

11.3 审核策划

11.3.1 审核时间

服务认证审核时间需结合 DSMM 成熟度级别、服务覆盖范围、组织规模三大核心要素测算，遵循 CNAS-CC105：2020《确定管理体系审核时间(QMS、EMS、OHSMS)》和 GB/T 27207-2020《合格评定 服务认证模式选择与应用导则》、GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》国家标准，确保时间预估科学、合规、可落地。

(1) 一阶段（服务管理）审核

根据申请组织的规模（组织人数、活动场所数量）不同，分为 1-3 人日，具体为：

1) 小型组织（组织人数≤50 人，单一场所）：0.5-1 个工作日

审核内容：服务认证申请材料、服务规范、质量手册、服务流程文件、投诉处理机制等。

2) 中型组织（组织人数 51-200 人，≤3 个场所）：1-2 个工作日

需额外审核场所间服务一致性文件、总部对各场所的管控制度。

3) 大型组织（组织人数＞200 人，＞3 个场所）：2-3 个工作日

增加区域服务差异分析、总部与场所的权责划分文件审核。

(2) 二阶段（服务特性）审核

1) 一阶段审核和二阶审核时间间隔最短不应少于 1 日，最长不应超过 6 个月。如需要更长的时间间隔，应重新实施第一阶段审核；

2) 整个审核时间中，现场审核时间不应少于总审核时间的 80%；

3) 现场审核人日数根据组织规模确定基准时间：

小型组织单一场所，基准时间为 2 人日；中型组织单一场所基准时间 3 人日；大型组织单一场所基准时间 5 人日。涉及多场所的人日数视具体情况适当调整。

4) 根据申请级别在基准时间基础上分为：1 级 2-6 人日，2 级 2-8 人日，3 级 4-10 人日，4 级 6-16 人日，5 级 6-20 人日。

(3) 监督审核

在初始的三年认证周期中，对特定组织实施监督审核的审核时间，宜与初次认证审核（第一阶段＋第二阶段）的时间成比例，即每年实施监督审核的总时间不少于初次认证审核时间的 1/3。监督审核时间通常情况下不会少于 1 个审核人日，否则可能影响审核有效性。

(4) 再认证

在考虑所有更新信息的基础上，再认证审核时间按照初次认证审核(第一阶段+第二阶段)时间的 2/3 计算。再认证审核时间通常情况下不会少于 1 个审核人日，否则可能影响审核有效性。

11.3.2 审查组的组成

(1) 认证机构应当充分考虑审核所涉及的人员能力、专业能力和公正性要求，确定审查组成员；

(2) 认证机构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核任务和责任；

(3) 技术专家主要负责提供认证审核的技术支持，不作为审查员实施审核，不计入审核时间，其在审核过程中的活动由审查组中的审查员承担责任；

(4) 审查组可以有实习审查员，其要在审查员的指导下参与审核，不计入审核时间，不单独出具记录等审核文件，其在审核过程中的活动由审查组中的审查员承担责任。

11.3.3 制定审核计划

(1) 制定审核计划，明确审核目的、审核范围、审核依据、审核时间及具体安排；

(2) 审查组应提前将审核计划告知申请组织，如遇特殊情况临时变更计划时，应及时将变更情况通知申请组织，并协商一致；

(3) 审查组在现场审核前应提前告知受审核方审查组成员信息，以便双方再次确认和解决可能存在的异议。

11.3.4 审核准备

(1) 审查组长应负责组织前期准备工作，包括制定审核方案、审核计划沟通、角色的指定、

任务分配、资源的申请；

(2) 审查组长应确保成员了解审核的方法、计划、申请组织的情况、审核中适用的工具等；

(3) 审查组成员根据分配的任务制定项目执行过程文档。

11.4 审核实施流程

11.4.1 一阶段（服务管理）审核实施

文档审核是第一阶段审核的核心环节，审查组需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。

编制一阶段审核报告，详细记录审核发现的问题和改进建议，为第二阶段的现场审核提供明确的方向和重点，确保整个审核过程的高效性和准确性。

11.4.2 二阶段（服务特性）审核实施

11.4.2.1 首次会议

审查组到达现场后，会同申请组织按照认证计划召开首次会议，申请组织的管理层和涉及到被审核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) 阐明审核的目的和准则；

(3) 确定审核日程安排；

(4) 介绍审核方法和程序；

(5) 确认审查组陪同人员、所需资源和设施；

(6) 说明审核结果的提交方法和可能存在的审核结论。

11.4.2.2 现场审核实施

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，适用时对数据安全能力持续建设和改进提出建议。

11.4.2.3 末次会议

审查组会同申请组织按照认证计划召开末次会议，申请组织的管理层和涉及到被审核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) 告知现场审核结论；

(2) 告知审核后续事项和发证流程；

(3) 告知如何获得证书后，到期换证、变更及年度监督审核的要求；

(4) 告知投诉、申诉程序。

如审查组长在本阶段审核中列出不符合项，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。

11.5 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。

11.6 审核报告

审查组长根据审查组的审核结果与内部讨论意见，负责编制审核报告。审核报告编制完成后，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核报告进行复核与批准，确保审核报告的权威性与有效性。

11.7 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，对审核报告、审核记录等进行复核的基础上，做出认证决定。同时，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核项目的认证决定；

(2) 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；

(3) 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。

11.8 认证证书的制作和发放

(1) 申请组织确认认证证书内容后，本机构完成证书制作和发放；

(2) 本机构在颁发认证证书后，当月数据应在次月 10 日前按照规定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（遇法定节假日不再顺延）。

12 获证后监督

12.1 监督审核周期

(1) 每年度进行一次监督审核，周期不超过 12 个月；

(2) 若超过期限未能实施监督审核的，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；

(3) 当本机构收到关于获证组织发生重大数据安全事故或组织结构、人员等方面发生重大变更等信息或投诉，并认为需要核实的，本机构可增加现场监督审核的频次。

12.2 监督审核决定

监督审核完成后，本机构根据监督审核情况和审核报告，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核结果。

13 再认证

(1) 认证证书期满前，若获证组织申请继续持有认证证书，应当至少在认证证书有效期结束前 3 个月向本机构提出申请，本机构按照本规则实施认证审核，并决定是否延续认证证书；

(2) 获证组织的获证服务未发生重大变化时，本机构可适当简化申请受理和资料审核程序；

(3) 对超过 3 个月仍未申请再认证的获证机构，应按初次认证进行实施；

(4) 因不可抗力或重大自然灾害的原因，不能在认证证书有效期内申请再认证的，获证组织应在证书有效期内向本机构提出书面申请说明原因。经本机构确认，再认证审核可在认证证书有效期后的 3 个月内实施，但不得超过 3 个月，在此期间本机构将暂停并收回已颁发的证书，同时获证机构也不得使用该认证证书。

14 认证证书和认证标志

14.1 认证证书管理要求

14.1.1 证书内容

(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核并经审核合格此证书方继续有效”的提示信息；

(8) 证书查询方式。除在本机构网站上公布认证证书的查询方式外，还应当在证书上注明："本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询"，以便于社会监督。

14.1.2 证书管理

本机构按照《认证证书和认证标志管理办法》，对获得认证的组织使用认证证书的情况实施有效跟踪调查，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；对撤销或者注销的认证证书予以收回；无法收回的，予以公布。获得认证的组织应当在广告、宣传等活动中正确使用认证证书和有关信息，任何组织不得利用数据安全能力成熟度认证证书和相关文字、符号误导公众认为其产品、管理体系通过认证。

14.2 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。

14.3 认证证书有效期

初次认证证书有效期最长为 3 年。再认证的认证证书有效期不超过最近一次有效认证证书截止期再加 3 年。

14.4 认证证书及认证标志样式

图 1：认证证书样式

图 2：认证证书副本样式

图 3：认证标志样式

15 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。

15.1 证书的保持

认证证书的保持需满足以下条件：

(1) 在规定的期限内按计划实施了监督，可证实体系运行持续有效并符合相应标准和认证要求、实施规则；

(2) 初次评价或上一次监督发现的不符合项纠正措施实施有效；

(3) 证书和标志的使用符合规定的要求；

(4) 按时缴纳规定的认证费用；

(5) 符合认证规定的其他要求。

本机构对于满足以上条件的获证组织将保持其注册资格，并以《保持使用认证证书和认证标志的通知》通知获证组织。

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，再认证的认证决定通过后，为获证组织换发新的认证证书。

15.2 证书的变更

15.2.1 当发生下列情况之一时，获证组织应向认证机构提交书面变更申请：

(1) 获证组织名称、注册地址、运营地址等变更；

(2) 认证机构规定的其他事项发生变更时，如认证范围、认证对象等。

15.2.2 当发生下列情况之一时，认证机构应通知获证组织换发认证证书：

(1) 认证依据变更，如认证依据标准发生修订或换版；

(2) 认证规则中涉及认证证书内容部分发生变更；

(3) 获证组织在本机构规定的时限内未能解决造成暂停的问题，本机构应缩小其认证范围。

15.3 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。

15.4.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。

16 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》。

17 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。

18 信息报送与公开

18.1 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。

18.2 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）