数据安全能力成熟度认证规则

中镡核信（上海）认证服务有限公司

版本号：V1.1　　发布日期：2024 年 10 月 25 日，实施日期：2024 年 11 月 1 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”）开展数据安全能力成熟度认证活动。

2 认证依据

以 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）为认证依据。

3 认证人员要求

认证审查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员注册资格。

认证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。

4 认证模式

初始现场文件审查+能力成熟度等级认证+获证后监督。

5 服务认证单元划分及认证分级

5.1 认证单元划分

数据安全能力成熟度认证以组织为单位，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。

5.2 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五级，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。

6 认证程序

6.1 认证申请

6.1.1 申请条件

1）应具有独立法人资格；

2）未列入国家信用信息严重失信主体相关名录；

3）从事行业有资质、资格要求的，应具备相关法定资质、资格。

6.1.2 申请组织提交的文件和材料

申请组织提供《数据安全能力成熟度（DSMM）认证申请书》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）数据安全相关认证、评估材料等；

5）拟申请的服务认证等级；；

6）其他有关资料。

6.2 受理认证申请

6.2.1 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：

- ◆ 认证要求明确、形成文件并得到理解；
- ◆ 本机构和申请组织之间在理解上的差异得到解决；
- ◆ 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。

6.2.2 签订认证合同

在实施认证审核之前，本机构将与认证申请组织订立具有法律效力的书面认证合同，以明确相关方的责任。

6.3 审核策划

6.3.1 审核时间

1）为确保认证审核的完整有效，认证机构应以附件 1《审核时间》所规定的审核时间为基础，根据申请组织所覆盖的活动范围、特性、技术复杂程度、认证要求和体系覆盖范围内的有效人数等情况，核算并拟定完成审核工作需要的时间。在特殊情况下，可以减少审核时间，但减少的时间不得超过附件 1 所规定的审核时间的 30%；

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%。

6.3.2 审核组的组成

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，确定审核组

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核组，必要时可以选择技术专家参加审核组。审核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核组中的审查员承担责任；

4）审核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核组中的审查员承担责任。

6.3.3 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）审核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）审核组在现场审核前应提前告知审核组成员信息，以便双方再次确认和解决可能存在的异议。

6.3.4 审核准备

1）审核组长应负责组织前期准备工作，包括计划沟通、角色的指定、任务分配、资源的申请；

2）审核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）审核组成员根据分配的任务制定检查表；

4）审核组全体成员签订《现场审查员公正性和保密性声明》（两份），分别由申请组织和本机构存档。

6.4 审核实施

6.4.1 数据能力成熟度认证过程

1）确定模型适用范围：分析需要保护的数据资产及业务范围，确定模型使用和认证范围；

2）确定能力成熟度级别目标：分析组织机构数据安全风险，确定能力成熟度等级建设目标；

3）选取数据安全过程域（PA）：针对申请组织的数据相关的业务现况，选取适当的数据安全 PA。对不适用于组织的数据安全 PA 或基本实践（BP）进行裁剪。例如，对于有的申请组织而言，不存在数据对外共享的处理，则无需选择共享数据安全的 PA；

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

5）确定申请组织整体等级：基于选择的数据安全 PA 范畴，结合所有 PA 的等级，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。

6.4.2 现场审核

6.4.2.1 首次会议

审核组到达现场后，会同申请组织按照认证程序召开首次会议，申请组织的管理层和数据安全相关的职能部门负责人员应参加会议。参会人员均应签到，审核组保留首次会议签到表，首次会议至少包含以下内容：

- ◆ 介绍审核组成员及其职责；
- ◆ 阐明审核的目的和准则；
- ◆ 确定审核日程安排；
- ◆ 介绍审核方法和程序；
- ◆ 确认审核组陪同人员、所需资源和设施；
- ◆ 说明审核结果的提交方法和可能存在的审核结论。

6.4.2.2 现场审核实施

审核组按照《现场认证审核计划》安排实施审核，通过人员访谈、文档审查、配置检查、工具测试和旁站式验证等方法进行审查，具体方法如下：

人员访谈：通过访谈的方式与被审核方进行交流、讨论等活动，获取相关证据，了解有关信息；

文档审查：审核组审查数据安全相关的文档材料是否涵盖完整数据生存周期的过程域和控制项，审查材料包括数据安全的制度规范流程、系统权限审批流程记录、数据发布审批流程记录等；

配置检查：根据申请组织提供的技术材料，登录相关的系统平台，检查核实其配置是否与技术材料保持一致；

工具测试：利用技术工具对系统平台进行测试，验证其是否符合数据安全成熟度模型特定等级的技术能力要求，可以采信具有等保测评机构资质等权威第三方机构的测试结论；

旁站式验证：审查人员在现场通过实地观察申请组织的人员行为、技术设施和环境状况

判定人员的安全意识、业务操作和管理程序等方面的安全情况。

6.4.2.3 末次会议

审核组会同申请组织按照认证程序召开末次会议，申请组织的管理层和数据安全相关的职能部门负责人员应参加会议。参会人员均应签到，审核组保留末次会议签到表，末次会议至少包含以下内容：

- 告知审核结论；
- 告知审核后续事项和发证流程；
- 告知如获得证书后，到期换证、变更及年度监督审核的要求；
- 告知投诉、申诉程序。

如审核组长在本阶段审核中列出不符合项和观察项（适用时），则需在该阶段末次会议中由申请组织现场签字确认，并要求申请组织在要求期限之内按照要求完成不符合项的纠正和采取纠正措施，并由审核组进行验证。审核组成员需及时向审核组长报告整改情况，由审核组长安排后续事宜。

6.5 不符合项的纠正和纠正措施及其结果的验证

1）对于审核中发现的不符合，审核组将出具《不符合项报告》。对于一般不符合，申请组织应在 1 个月内分析原因，并说明为消除不符合已采取或拟采取的具体纠正和纠正措施。

2）本机构将对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证。对于严重不符合，申请组织应在 3 个月内采取纠正和纠正措施，本机构将对纠正和纠正措施作现场验证。

6.6 审核报告

1）审核组长负责编写《认证审核报告》初稿，给出初步结论；

2）审核组长组织报告内容讨论，形成报告终稿；

3）《认证审核报告》需要经由审核组长和申请组织代表共同确认。

6.7 认证决定

1）审核组长提交审核报告、审核记录到本机构；

2）认证决定与复核人员依据 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、审核记录等进行综合评价的基础上，做出认证决定。同时，认证决定与复核人员为本机构管理控制下的人员，审核组成员不得参与对审核项目的认证决定；

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

4）申请人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。

6.8 认证证书的制作和发放

1）申请方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，应在 30 个工作日内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。

7 获证后监督

7.1 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。

7.2 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。

8 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，由本机构按照认证程序，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 个月仍不能复审的获证机构，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复审的，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，复审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。

9 认证证书和认证标志

9.1 认证证书应至少包含以下信息：

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。除公布认证证书在本机构网站上的查询方式外，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。

9.2 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。

9.3 认证证书及认证标志样式

图 1：认证证书样式

图 2：认证标志样式

10 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和认证人日计算办法参考，具体参见 《收费管理办法》和《审核时间》。

11 信息报送与公开

11.1 信息报送

认证机构在颁发认证证书后，应当在 30 个工作日内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。

11.2 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》和《公正性承诺》。

附件 1《审核时间》

申请等级	初次认证/再认证文件审查人日	初次认证/再认证现场审核人日	监督现场审核人日
1	1	3	2
2	1	5	3
3	1	7	5
4	2	8	6
5	2	10	8

注：

1、此为最低参考时间，具体审核时间需结合实际企业规模、企业人员数量、数据规模、审核范围等因素规划；

2、此为实际工作时间，不包含审核组往返申请组织所在地时间。