编号：CESI-SC-OD11

数据安全能力成熟度服务认证规则
1.4

2025-6-13 发布　　2025-6-13 实施

北京赛西认证有限责任公司

前 言

本规则依据《中华人民共和国认证认可条例》制定。本规则明确了对组织数据安全能力成熟度进行认证的基本原则和要求。

目　录

1 适用范围

本规则规定了对组织数据安全能力成熟度进行认证的基本原则和要求。

认证领域或技术领域划分：SC11。

2 认证依据

GB/T37988-2019《信息安全技术 数据安全能力成熟度模型》

3 认证模式

服务特性检验+服务管理审核+获证后监督

4 认证实施

4.1. 认证申请

4.1.1 申请范围界定

场所：认证申请方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。

活动：认证申请方申请的业务过程或系统的数据处理活动。

等级：认证申请方申请的 GB/T37988-2019 中的数据安全能力成熟度等级。

4.1.2 申请时需提交的文件资料

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价表；

4) 其他认证所需相关材料。

4.2. 申请评审

认证机构在 5 个工作日内对申请材料进行评审，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）告知认证申请方。

若决定受理，认证机构根据认证申请资料确定认证方案，并通知认证申请方。

4.3. 认证评价

认证机构对组织的数据安全能力实施服务特性检验、服务管理审核，并出具报告。

服务管理审核和服务特性检验依据 GB/T37988-2019《信息安全技术 数据安全能力成熟度模型》开展。

4.4. 复核、认证决定

认证机构应对认证相关的所有信息包括申请评审、评价过程和结论进行复核。

认证机构根据评价、复核以及其他相关的所有信息做出认证决定。

对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证申请方限期整改，整改后仍不符合的，以书面形式通知认证申请方终止认证。

4.5. 获证后监督

4.5.1. 监督的频次和方式

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，年度监督审核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决定日期起 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。

4.5.2. 监督的内容

监督时至少应评价以下内容：

（1）上次评价以来组织活动及运行的资源是否有变更；

（2）组织数据安全特性有关的活动是否有效运行；

（3）涉及法律法规规定的，相关法律法规或技术标准是发生变化，是否持续符合相关规定；

（4）数据安全能力是否持续保持；

（5）获证组织对认证标志的使用或对认证资格的引用是否符合相关的规定；

（6）是否及时接受和处理投诉；

（7）针对投诉的问题，及时制定并实施了有效的持续改进。

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。

4.5.3. 获证后监督结果的评价

认证机构对证后监督报告和其他相关资料信息进行综合评价，监督结果符合要求的，可保持认证资格，继续使用认证证书和认证标志；对监督复查时发现的不符合项应在认证机构规定期限内完成纠正措施。逾期按认证机构公开文件《服务认证程序规则》的要求执行，并对外公告。

4.6. 再认证

认证机构在认证证书到期前对获证机构进行再认证，再认证过程与初次认证保持一致，再认证条款与初次认证相同。

4.7. 认证时限

认证时限是指自作出受理决定之日起至作出认证决定所实际发生的工作日，一般为 60 个工作日（不包含整改时间）。（时限按项目实际描述，每个项目可能不同）

5 认证证书

获证组织必须按认证机构公开文件《服务认证程序规则》的要求使用认证证书。

5.1. 证书的保持

认证证书有效期为 3 年（可按项目实际规定）。在有效期内，通过认证机构的获证后监督，保持认证证书的有效性。

证书到期需延续使用的，获证组织应当在有效期届满前 6 个月内提出认证申请。认证机构应当采用再认证的方式，对符合认证要求的申请换发新证书。

5.2. 证书的变更

认证证书有效期内，获证组织名称、地址，或认证评价内容等发生变化时，获证组织应当向认证机构提出变更申请。认证机构根据变更的内容，对变更申请资料进行评价，确定是否批准变更。如需进行认证评价，还应当在批准变更前进行认证评价。当认证要求（如

标准）发生变化时，获证组织应按规定换证，未按规定换发的认证证书自行失效，同时认证机构应予以撤销证书，要求其停止使用认证标志。

认证的变更按照认证机构公开文件《服务认证程序规则》的要求执行。

5.3. 认证的暂停、撤销和注销

当获得认证组织不再符合认证要求时，认证机构对认证证书予以暂停直至撤销，要求其停止使用认证标志。认证申请方在认证证书有效期内可申请暂停或注销认证证书。认证机构采用适当方式对外公布被暂停、注销和撤销的认证证书。

暂停期限为 6 个月。暂停期限内，获证机构可提出恢复认证的申请，经认证机构评审、批准后，方可使用该证书。在暂停认证期间，获证机构不得继续使用证书和认证标志。暂停期满仍未恢复认证资格的，认证证书自动撤销。

认证的暂停、恢复、撤销、注销及涉及的认证证书和标志使用的具体要求按照认证机构公开文件《服务认证程序规则》执行。

6 认证标志

在认证证书有效期内， 获证组织应当按照规定在广告等宣传中正确使用认证证书和认证标志，不得对公众产生误导。

获证组织必须按认证机构公开文件《服务认证程序规则》的要求使用认证标志。

（如果有特殊的或具体的要求，公开文件中没有明确提及的，可以增加内容。）

7.1 准许使用的认证标志样式

（以下内容请按实际写）

1）认证标志样式：

2) 规格：标志图案的尺寸长宽比例 1:1，允许线性比例缩放。

3) 颜色：应使用基本颜色或单一黑色。

7.2 变形认证标志的使用

本规则覆盖的产品不允许使用任何形式的变形认证标志。

7.3 加施方式及位置

获证组织可在通过认证的系统、相关宣传材料上加施认证标志。