编号：CESI-SC-OD11A

数据处理活动安全服务认证规则
V1.0

2026-10-29 发布　　2026-10-29 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处理活动安全服务能力进行认证的基本原则和要求。

本实施规则由北京赛西认证有限责任公司制订并发布，版权归北京赛西认证有限责任公司所有，任何组织及个人未经北京赛西认证有限责任公司许可，不得以任何形式全部或部分使用。本规则的最终解释权归北京赛西认证有限责任公司所有。

本规则首次发布日期：2026.10.29，实施日期：2026.10.29。

目　录

1 适用范围 4
2 认证依据 4
3 认证模式 4
4 领域划分 4
5 认证程序 4
5.1. 认证申请 4
5.1.1. 受理认证申请的条件 5
5.1.2. 申请范围界定 5
5.1.3. 申请时需提交的文件资料 5
5.2. 申请评审与认证合同 6
5.3. 认证评价 6
5.3.1. 审核时间 6
5.3.2. 组建审查组 7
5.3.3. 现场评价 7
5.3.4. 服务特性测评 9
5.3.5. 服务管理审核 11
5.3.6. 评价内容 13
5.3.7. 评价方法 13
5.3.8. 评价结论 14
5.3.9. 评价报告 14
5.4. 复核、认证决定 14
5.5. 保持认证 15
5.5.1. 保持认证的条件 15
5.5.2. 监督的频次和方式 16
5.5.3. 监督的内容 16
5.5.4. 获证后监督结果的评价 17
5.5.5. 证书有效期内的情况通报 17
5.5.6. 影响认证的变更 17
5.5.7. 扩大认证范围 18
5.5.8. 缩小认证范围 18
5.5.9. 认证要求的变更 19

5.6. 再认证 19
5.7. 认证时限 20
6 认证证书 20
6.1. 证书的保持 20
6.2. 证书的变更 21
6.3. 认证的暂停、撤销和注销 21
6.3.1. 暂停 21
6.3.2. 撤销 22
6.3.3. 暂停、撤销的公示 23
7 认证标志 23
8 证书和标志的使用 24
9 申诉、投诉 25
附录 A 证书模板 26
附录 B CESI 认证业务联系方式 27

1 适用范围

本规则规定了对组织数据安全能力（组织向其内部提供的数据处理活动安全服务能力）进行认证的基本原则和要求，包括数据采集安全、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、通用安全要求。

本规则服务认证的领域为：SC12“电信服务；信息检索和提供服务”。

2 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》

注：GB/T 37988-2019 的技术工具条款规定了组织向其内部提供数据处理活动安全服务的服务要求，是服务特性测评依据。GB/T 37988-2019 的组织建设、制度流程、人员能力条款规定了组织向其内部提供数据处理活动安全服务的管理要求，是服务管理审核依据。

3 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。

具体选用以下服务认证模式，实现服务特性测评：

1）公开服务特性检验，简称模式 A；

2）服务能力确认或验证，简称模式 G；

选用以下服务认证模式，实现服务管理审核：

3）服务能力确认或验证，简称模式 G；

4）服务管理审核，简称模式 I。

初次认证/监督评价/再认证时，均选用模式 A+模式 G+模式 I。

注：根据 GB/T27207《合格评定服务模式与应用导则》可选择的认证模式包括 a)公开服务特性检验（模式 A）、b)神秘顾客检验（模式 B）、c)公开的服务特性检测（模式 C）、d)神秘顾客检测（模式 D）、e)顾客调查（模式 E）、f)既往服务足迹检测（模式 F）、g)服务能力确认或验证（模式 G）、h) 服务设计审核（模式 H）、i) 服务管理审核（模式 I）。

4 领域划分

单一领域：数据处理活动安全服务。

5 认证程序

5.1. 认证申请

5.1.1. 受理认证申请的条件

申请方可以是：

a. 研发或提供服务的组织；

b. 对提供服务的组织有控制权的机构；

申请方应具备的基本条件是：

a. 申请方应具有明确的法律地位。如申请方为一法律实体的一部分，应有证据表明申请方能独立承担法律责任；

b. 遵守本规则和相应服务认证规则的要求；

c. 当前未被行政监管部门责令停产停业整顿；

当前未列入“国家企业信用信息公示系统”和“信用中国”发布的严重违法失信名单。

5.1.2. 申请范围界定

场所：认证申请方对其业务过程或系统提供数据处理活动安全服务的物理场所。

活动：认证申请方申请的业务过程或系统的数据处理活动。

星级：认证申请方申请的业务过程或系统的数据处理活动安全服务能力星级。

数据处理活动安全服务能力星级定义如下表所示：

星级名称	星级定义
一星级	非正式执行：随机、无序、被动地执行安全过程，依赖于个人经验，无法复制。
二星级	计划跟踪：在业务系统级别主动地实现了安全过程的计划与执行，但没有 形成体系化。
三星级	充分定义：在组织级别实现了安全过程的规范执行。
四星级	量化控制：建立了量化目标，安全过程可度量。
五星级	持续优化：根据组织的整体目标，不断改进和优化安全过程。

5.1.3. 申请时需提交的文件资料

认证申请人应向认证机构提交的材料包括但不限于：

1) 认证申请书；

2) 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；

3) 国家企业信用信息公示系统年度报告电子版；

4) 数据安全能力成熟度自评价表；

5) 其他认证所需相关材料。

5.2. 申请评审与认证合同

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。

通过申请评审的，赛西认证应与认证申请人签订具有法律效力的认证合同，明确认证服务的费用、付费方式和违约条款，及认证申请人、赛西认证和获证组织的责任。认证费用应由认证申请人向赛西认证直接支付。

5.3. 认证评价

本领域服务认证包括初次认证审查、获证后的监督审查、认证到期前的再认证审查和特殊审查（适用时）。

认证机构对数据处理活动安全服务实施服务特性测评、服务管理审核，并出具报告。

初次认证、再认证评价应在申请组织申请认证的范围涉及到的各个场所现场进行。对具有一个以上场所的组织的服务认证，初次认证在组织认证范围内的每个场所进行。如果组织不同的场所以相似的方式进行认证覆盖的活动，且这些活动都处于该申请组织授权和控制下，可以基于以往服务认证的结果，在监督活动中对这些场所进行抽样。

为使现场评价活动能够观察到服务活动情况，应安排在认证范围覆盖的服务活动正常运行时进行。审查组在编制审查计划时，应当充分考虑服务正常运行时段和风险时段，确保现场审查活动能捕捉到服务最真实的运行状态。

5.3.1. 审核时间

现场审查人日数（1 人日为 8 小时）如下表所示：

申请	初次认证现	初次认证现	监督现场评	监督现场评	再认证现场评	再认证现场评

星级	场评价人日（服务特性测评）	场评价人日（服务管理审核）	价人日（服务特性测评）	价人日（服务管理审核）	价人日[注1]（服务特性测评）	价人日[注1]（服务管理审核）
一星级	2	2	1	1	2	2
二星级	3	2	1.5	1	3	2
三星级	4	2	2	1	4	2
四星级	4	3	2	1.5	4	3
五星级	5	3	2.5	1.5	5	3

5.3.2. 组建审查组

由赛西认证选派有资格的审查人员组成审查组（一般不少于 1 人组成）。必要时可聘请技术专家参加。派出技术专家、观察员和实习审核员时，上述三类人员不得独立开展服务认证审查活动，也不计入现场审查人日数。

审查人员应取得国家认监委确定的认证人员注册机构批准的服务认证审查员注册资格。审查人员应接受“数据处理活动安全服务认证”培训，并经过该领域专业能力评价。

审查组长从该领域的合格审查人员里选拔。

5.3.3. 现场评价

由赛西认证选派有资格的审查员组成审查组对申请方认证范围内的场所进行现场评价。必要时可聘请技术专家参加。

1、现场评价开始时，首先召开首次会议，受评价方关键岗位人员（最高管理者或管理者代表，或书面授权的其他高级管理层成员；受审查部门（服务过程涉及的部门）负责人）应参加会议。审查组在首次会议上向受审查方说明评价目的、评价依据、评价覆盖范围和评价方法、明确受限制区域，确认评价计划，同时将可能引起评价中止的条件告知受审核方。如双方有不同意见，应协商解决。

2. 审查组根据评价计划及现场评价记录单，采用会晤、访问、查阅文件记录、现场观察等方法，对受评价方的服务能力进行审查，取得客观证据，并记录审查结果。

3. 在审查期间，受评价方应予协助、配合，并保证：

a）审查组能够查阅组织服务能力有关的文件资料和质量记录，包括原始记录；

b）审查组能够进入与服务能力审查有关的场所；

c）审查组能够与服务能力体系有关的人员进行访谈；

d）提供审查组进行服务能力审查时所必需的设施和条件，并指定陪同人员。

e）观察员（如行业监督部门委派）的参与。

4. 现场审查结束前，审查组应与受评价方负责人（或其代表）进行会晤，表明审查组现场评价的意见。并召开末次会议，表明审查组现场评价的结论意见。

现场评价结论包括下列情况：

- 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。

5. 受评价方如对结论意见有不同看法，与审查组不能达成一致时，审查组应专门加以记录并报告赛西认证。

6. 发生下列情况的，审查组应向赛西认证报告后终止审核：（1）认证申请人对审查活动不予配合，审查活动无法进行；（2）认证申请人的最高管理者或经授权的高级管理层成员缺席首、末次会议；（3）认证申请人实际情况与申请材料有重大不一致；（4）其他导致审查程序无法完成的情况。

对于现场评价结论，组长有最后决定权。受评价方应针对评价中发现的不符合项，按照赛西认证规定的时间要求制定并实施有效的纠正和纠正措施，审查组进行验证。纠正措施的验证有书面验证，现场跟踪验证验证两种方式。由审查组根据受评价方不符合项的性质和纠正措施的要求确定其中一种有效的验证方式。

受评价方完成整改并上报审查组长后，由审查组长验证纠正及纠正措施的有效性，完成评价报告，上报赛西认证。

5.3.4. 服务特性测评

服务特性测评以公开服务特性检验（模式 A）+服务能力确认或验证（模式 G）方式开展。

公开服务特性检验、服务能力确认或验证均依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》开展。

服务特性测评由认证机构委派具有服务认证资质的专业审查员依据 GB/T 37988-2019 对与申请方数据处理活动安全服务能力相关的数据安全技术条款（技术工具）进行审查。

认证机构也可以委托评估机构依据 GB/T37988-2019 对组织的数据安全能力相关的技术工具要求进行服务特性检验（模式 A），出具服务特性检验报告（即：数据安全能力成熟度评估报告）。

评价方法如下：

a. 参考 GB/T37988-2019 的“附录 C 能力成熟度等级评估流程和模型使用方法”，针对受评价方数据处理活动相关的业务现况，从适用于该组织业务的 PA 里，选取技术工具类 BP；

b. 服务特性测评依据如下表所示：

PA	1 级	2 级	3 级	4 级	5 级
数据分类分级	/	/	6.1.2.3	6.1.2.3+6.1.2.4	6.1.2.3+6.1.2.4+6.1.2.5
数据采集安全管理	/	/	6.2.2.3	6.2.2.3+6.2.2.4	6.2.2.3+6.2.2.4+6.2.2.5
数据源鉴别及记录	/	6.3.2.2	6.3.2.3	6.3.2.3+6.3.2.4	6.3.2.3+6.3.2.4+6.3.2.5
数据质量管理	/	/	6.4.2.3	6.4.2.3	6.4.2.3+6.4.2.4+6.4.2.5
数据传输加密	/	7.1.2.2	7.1.2.3	7.1.2.3+7.1.2.4	7.1.2.3+7.1.2.4+7.1.2.5
网络可用性管理	/	/	7.2.2.3	7.2.2.3+7.2.2.4	7.2.2.3+7.2.2.4+7.2.2.5
存储媒体安全	/	/	8.1.2.3	8.1.2.3+8.1.2.4	8.1.2.3+8.1.2.4+8.1.2.5

逻辑存储安全	/	8.2.2.2	8.2.2.3	8.2.2.3+8.2.2.4	8.2.2.3+8.2.2.4+8.2.2.5
数据备份和恢复	/	8.3.2.2	8.3.2.3	8.3.2.3+8.3.2.4	8.3.2.3+8.3.2.4+8.3.2.5
数据脱敏	/	9.1.2.2	9.1.2.3	9.1.2.3+9.1.2.4	9.1.2.3+9.1.2.4+9.1.2.5
数据分析安全	/	/	9.2.2.3	9.2.2.3+9.2.2.4	9.2.2.3+9.2.2.4+9.2.2.5
数据正当使用	/	/	9.3.2.3	9.3.2.3+9.3.2.4	9.3.2.3+9.3.2.4+9.3.2.5
数据处理环境安全	/	9.4.2.2	9.4.2.3	9.4.2.3+9.4.2.4	9.4.2.3+9.4.2.4+9.4.2.5
数据导入导出安全	/	9.5.2.2	9.5.2.3	9.5.2.3+9.5.2.4	9.5.2.3+9.5.2.4+9.5.2.5
数据共享安全	/	/	10.1.2.3	10.1.2.3+10.1.2.4	10.1.2.3+10.1.2.4+10.1.2.5
数据发布安全	/	/	10.2.2.3	10.2.2.3+10.2.2.4	10.2.2.3+10.2.2.4+10.2.2.5
数据接口安全	/	10.3.2.2	10.3.2.3	10.3.2.3+10.3.2.4	10.3.2.3+10.3.2.4+10.3.2.5
数据销毁处置	/	11.1.2.2	11.1.2.3	11.1.2.3+11.1.2.4	11.1.2.3+11.1.2.4+11.1.2.5
存储媒体销毁处置	/	11.2.2.2	11.2.2.3	11.2.2.3+11.2.2.4	11.2.2.3+11.2.2.4+11.2.2.5
数据安全策略规划	/	/	12.1.2.3	12.1.2.3	12.1.2.3+12.1.2.4+12.1.2.5
组织和人员管理	/	/	12.2.2.3	12.2.2.3+12.2.2.4	12.2.2.3+12.2.2.4+12.2.2.5
合规管理	/	/	12.3.2.3	12.3.2.3+12.3.2.4	12.3.2.3+12.3.2.4+12.3.2.5
数据资产管理	/	/	12.4.2.3	12.4.2.3+12.4.2.4	12.4.2.3+12.4.2.4+12.4.2.5
数据供应链安全	/	/	12.5.2.3	12.5.2.3+12.5.2.4	12.5.2.3+12.5.2.4+12.5.2.5
元数据管理	/	/	12.6.2.3	12.6.2.3+12.6.2.4	12.6.2.3+12.6.2.4+12.6.2.5
终端数据安全	/	12.7.2.2	12.7.2.3	12.7.2.3+12.7.2.4	12.7.2.3+12.7.2.4+12.7.2.5
监控与审计	/	/	12.8.2.3	12.8.2.3+12.8.2.4	12.8.2.3+12.8.2.4+12.8.2.5
鉴别与访问控制	/	12.9.2.2	12.9.2.3	12.9.2.3+12.9.2.4	12.9.2.3+12.9.2.4+12.9.2.5
需求分析	/	/	12.10.2.3	12.10.2.3	12.10.2.3+12.10.2.4+12.10.2.5
安全事件应急	/	/	12.11.2.3	12.11.2.3+12.11.2.4	12.11.2.3+12.11.2.4+12.11.2.5

c. 依据组织申请评估的星级，依据上表，评估该等级技术工具 BP 要求满足情况。

5.3.5. 服务管理审核

服务管理审核以服务能力确认或验证（模式 G）+服务管理审核（模式 I）方式开展。

服务能力确认或验证、服务管理审核均依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》开展，以确定服务流程管理是否符合要求。

服务管理审核由认证机构委派具有服务认证资质的专业审查员依据 GB/T 37988-2019 对与申请方数据处理活动安全服务能力相关的数据安全管理条款（组织建设、制度流程、人员能力）进行审查，并出具《服务认证审查报告》。

评价方法如下：

d. 参考 GB/T37988-2019 的“附录 C 能力成熟度等级评估流程和模型使用方法”，针对受评价方数据处理活动相关的业务现况，从适用于该组织业务的 PA 里，选取组织建设、制度流程、人员能力类 BP；

e. 服务管理审核依据如下表所示：

PA	1 级	2 级	3 级	4 级	5 级
数据分类分级	6.1.2.1	6.1.2.2	6.1.2.3	6.1.2.3	6.1.2.3+6.1.2.5
数据采集安全管理	6.2.2.1	6.2.2.2	6.2.2.3	6.2.2.3+6.2.2.4	6.2.2.3+6.2.2.4+6.2.2.5
数据源鉴别及记录	6.3.2.1	6.3.2.2	6.3.2.3	6.3.2.3+6.3.2.4	6.3.2.3+6.3.2.4+6.3.2.5
数据质量管理	6.4.2.1	6.4.2.2	6.4.2.3	6.4.2.3+6.4.2.4	6.4.2.3+6.4.2.4+6.4.2.5
数据传输加密	7.1.2.1	7.1.2.2	7.1.2.3	7.1.2.3+7.1.2.4	7.1.2.3+7.1.2.4
网络可用性管理	7.2.2.1	7.2.2.2	7.2.2.3	7.2.2.3	7.2.2.3
存储媒体安全	8.1.2.1	8.1.2.2	8.1.2.3	8.1.2.3	8.1.2.3
逻辑存储安全	8.2.2.1	8.2.2.2	8.2.2.3	8.2.2.3+8.2.2.4	8.2.2.3+8.2.2.4+8.2.2.5

数据备份和恢复	8.3.2.1	8.3.2.2	8.3.2.3	8.3.2.3+8.3.2.4	8.3.2.3+8.3.2.4+8.3.2.5
数据脱敏	9.1.2.1	9.1.2.2	9.1.2.3	9.1.2.3+9.1.2.4	9.1.2.3+9.1.2.4
数据分析安全	9.2.2.1	9.2.2.2	9.2.2.3	9.2.2.3	9.2.2.3+9.2.2.5
数据正当使用	9.3.2.1	9.3.2.2	9.3.2.3	9.3.2.3+9.3.2.4	9.3.2.3+9.3.2.4
数据处理环境安全	9.4.2.1	9.4.2.2	9.4.2.3	9.4.2.3+9.4.2.4	9.4.2.3+9.4.2.4+9.4.2.5
数据导入导出安全	9.5.2.1	9.5.2.2	9.5.2.3	9.5.2.3	9.5.2.3+9.5.2.5
数据共享安全	10.1.2.1	10.1.2.2	10.1.2.3	10.1.2.3+10.1.2.4	10.1.2.3+10.1.2.4+10.1.2.5
数据发布安全	10.2.2.1	10.2.2.2	10.2.2.3	10.2.2.3+10.2.2.4	10.2.2.3+10.2.2.4
数据接口安全	10.3.2.1	10.3.2.2	10.3.2.3	10.3.2.3	10.3.2.3
数据销毁处置	11.1.2.1	11.1.2.2	11.1.2.3	11.1.2.3+11.1.2.4	11.1.2.3+11.1.2.4+11.1.2.5
存储媒体销毁处置	11.2.2.1	11.2.2.2	11.2.2.3	11.2.2.3+11.2.2.4	11.2.2.3+11.2.2.4+11.2.2.5
数据安全策略规划	12.1.2.1	12.1.2.2	12.1.2.3	12.1.2.3+12.1.2.4	12.1.2.3+12.1.2.4+12.1.2.5
组织和人员管理	12.2.2.1	12.2.2.2	12.2.2.3	12.2.2.3+12.2.2.4	12.2.2.3+12.2.2.4+12.2.2.5
合规管理	12.3.2.1	12.3.2.2	12.3.2.3	12.3.2.3+12.3.2.4	12.3.2.3+12.3.2.4+12.3.2.5
数据资产管理	12.4.2.1	12.4.2.2	12.4.2.3	12.4.2.3+12.4.2.4	12.4.2.3+12.4.2.4+12.4.2.5
数据供应链安全	12.5.2.1	12.5.2.2	12.5.2.3	12.5.2.3+12.5.2.4	12.5.2.3+12.5.2.4+12.5.2.5
元数据管理	12.6.2.1	12.6.2.2	12.6.2.3	12.6.2.3+12.6.2.4	12.6.2.3+12.6.2.4
终端数据安全	12.7.2.1	12.7.2.2	12.7.2.3	12.7.2.3+12.7.2.4	12.7.2.3+12.7.2.4
监控与审计	12.8.2.1	12.8.2.2	12.8.2.3	12.8.2.3+12.8.2.4	12.8.2.3+12.8.2.4
鉴别与访问控制	12.9.2.1	12.9.2.2	12.9.2.3	12.9.2.3+12.9.2.4	12.9.2.3+12.9.2.4
需求分析	12.10.2.1	12.10.2.2	12.10.2.3	12.10.2.3+12.10.2.4	12.10.2.3+12.10.2.4+12.10.2.5
安全事件应急	12.11.2.1	12.11.2.2	12.11.2.3	12.11.2.3	12.11.2.3+12.11.2.5

f. 依据组织申请评估的星级，依据上表，评估该星级组织建设、制度流程、人员能力 BP 要求满足情况。

5.3.6. 评价内容

初次认证时，依据申请方申请 GB/T37988-2019 的能力成熟度星级和服务特性检验报告，到申请范围内的数据处理活动所在场所现场，对该星级各个过程域“组织建设、制度流程和人员能力”等服务管理要求进行审查。

现场评价重点是审查申请方符合 GB/T37988-2019《信息安全技术 数据安全能力成熟度模型》的情况，基于服务特性检验报告建议的星级进行审查。

5.3.7. 评价方法

组织机构的数据处理活动安全服务能力星级取决于各个数据安全 PA 的能力成熟度等级。各个数据安全 PA 的成熟度等级取决于该 PA 中的 BP 对于目标等级的满足情况。

综合判定方法：

（一）单个 PA 的满足判定。

BP 满足率 =（X-Y-Z）÷（X-Y）×100%

X：PA 下的全部 BP 数。

Y：PA 下组织不适用的 BP 数。

Z：PA 下组织不满足的 BP 数。

当 BP 满足率≥80%时，该 PA 满足。

（二）数据处理活动安全服务能力星级判定。

PA 满足率 =（M-N-P）÷（M-N）×100%

M：30（总 PA 数）。

N：组织不适用的 PA 数。

P：组织不满足的 PA 数。

当 PA 满足率≥80%时，该数据处理活动安全服务能力星级达到。

说明：组织适用的 PA 数应≥28 个。

5.3.8. 评价结论

审查组以审查报告的形式向认证机构报告评价结论。评价结论：

- 达到申请组织申请的数据处理活动安全服务能力星级，推荐注册；
- 未达到申请组织申请的数据处理活动安全服务能力星级，不推荐注册。

5.3.9. 评价报告

审查组以评价报告的形式向认证机构报告评价结论。依据服务特性测评和服务管理审查的综合评价，出具推荐或不推荐符合对应级别的结论。

审查组应为每次评价活动提供书面报告，报告应包括但不限于以下内容：

a）评价的目的、范围和准则；

b）申请方的基本情况（包括名称、地址等）；

c）本次评价覆盖的认证单元；

d）抽样及样本信息；

e）评价结果及其说明；

f）与有关认证要求符合性的陈述（包括任何不符合）；

g）报告覆盖的时间段；

h）结论。

5.4. 复核、认证决定

赛西认证在收到审查组提交的全套评价资料后，交赛西认证技术委员会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，并根据评价、复核以及其他相关的所有信息，在 20 个工作日内做出认证决定。

获准认证的申请方，应符合下列条件：

a. 与赛西认证签署了正式服务认证合同，满足申请方条件（见 5.1.1）；

b. 从事的服务活动符合相关法律法规的规定，在认证过程中履行了应尽责任和义务；

c. 认证评价程序符合规定要求，认证资料完整、手续齐全；

d. 服务经评价符合相应认证标准、服务认证规则要求，对赛西认证评价时提出的不符合项已按要求全部完成了纠正措施并经审查组验证符合要求。

e. 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。

对暂不符合认证要求的，可要求认证申请方限期整改。

整改后仍不满足上述要求，评定该受评价方不符合认证要求，客户部以书面形式告知受评价方并说明其未通过认证的原因。

评价结果符合申请认证标准要求的，赛西认证将向申请方提供书面评价报告以及由赛西认证总经理签发的赛西认证相关服务认证证书，证书有效期见相应认证实施规则要求。

赛西认证在机构网站上发布赛西认证服务认证合格组织名录，用以向社会各界证实认证合格组织符合有关认证标准的要求，同时为用户与获证组织建立合同关系提供选择指南。

赛西认证利用各种机会向社会用户介绍相关的服务认证合格组织，并接受用户对有关情况的查询。

5.5. 保持认证

5.5.1. 保持认证的条件

服务认证证书获准保持应符合下列条件：

a. 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；

b. 按认证实施规则规定的周期和程序接受监督审查并符合要求；

c. 认证证书和认证标志的使用符合赛西认证规定的要求；

d. 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；

e. 按规定要求及时向赛西认证报告相关变更情况；

f. 按规定要求按时缴纳认证监督费用；

g. 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。

5.5.2. 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。

5.5.3. 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 1/2，两次监督需覆盖“认证依据”全部条款。

5.5.4. 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。

5.5.5. 证书有效期内的情况通报

获证组织发生以下情况时，需及时联系赛西认证，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 个月内通知赛西认证客户服务部，如发生上述 a、b 条情况时，应在事故或问题发生后 48 小时内通知赛西认证客户服务部（特殊情况不超过 1 周）。赛西认证根据情况决定是否进行调查，涉及变更的按本文件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；或按本文件做出认证暂停、撤销的决定。

5.5.6. 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。

赛西认证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核查、公开服务特性检验、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。

5.5.7. 扩大认证范围

扩大认证范围包括服务覆盖的场所范围的扩大，服务活动的增加（适用时）。

5.5.7.1 扩大认证范围的条件

a. 获证组织申请扩大认证范围应在其法律地位文件和资质规定的范围内；

b. 获证组织的服务应覆盖申请扩大的认证范围，并符合认证标准要求；

c. 至少近一年来，获证组织在申请扩大认证范围内未发生重大事故和国家检查不合格；

5.5.7.2 扩大认证范围的程序

a. 获证组织需向赛西认证正式提交扩大认证范围的书面申请书和相关附件；

b. 赛西认证对获证组织的扩项申请进行评审，适用时获证组织应与赛西认证补充签署或修订认证合同，并按照规定补充缴纳认证费用；

c. 获证组织申请扩大认证范围所涉及的服务文件进行审查，服务特性测评（适用时）符合认证标准；

d. 对获证组织申请扩大认证范围所涉及的服务，赛西认证结合监督审查或按协议要求实施认证程序，对认证合格者按初审程序更换证书。

5.5.8. 缩小认证范围

5.5.8.1 缩小认证范围的条件

如果组织在认证范围的某些部分持续地或严重地不满足认证要求，赛西认证将缩小其认证范围，以排除不满足要求的部分，具体情况如下：

a ． 获证组织的认证范围内部分服务范围、服务场所、区域等不再继续符合认证标准和其他附加要求；或

b. 获证组织的认证范围内部分服务范围、服务场所、区域等不愿再继续保持认证资格的。

5.5.8.2 缩小认证范围的程序

a. 获证组织向赛西认证正式提交缩小认证范围的书面申请书，并提供理由和证据；

b. 需要时，获证组织与赛西认证修订认证合同；

c. 经赛西认证技术委员会评定，认为获证组织在申请缩小认证范围不会对仍需保持的认证范围产生影响，赛西认证批准换发认证证书，但认证证书的注册号和有效期保持不变。

5.5.9. 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，赛西认证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赛西认证补充签署或修订认证合同。

5.6. 再认证

认证合格证书有效期满前三个月，获证组织可提出换证申请。赛西认证将对获证组织服务进行全面再认证，全面再认证的程序与初次认证时的程序相同。经全面再认证确认获证组织服务持续满足认证标准要求，赛西认证批准同意其延长，并更换证书。

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。

5.7. 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，其中包括服务特性检验时间、文件审查时间、服务管理审核时间、认证结果评价和批准时间、证书制作时间。

评估机构对服务特性检验时间一般为 7-20 个工作日（根据企业业务系统及数据活动复杂性不同浮动，评估后出具评估报告时间一般为 10 个工作日）。

服务管理审核后提交报告时间一般为 5 个工作日，以审查员完成现场审查，收到企业递交的不合格纠正措施报告之日起计算。

认证结果评价和批准时间、证书制作时间一般不超过 5 个工作日。

6 认证证书

服务认证证书（见附录 A）由赛西认证依据在国家认监委（CNCA）备案的证书要求进行统一制作、发放。未经赛西认证授权，其他组织或个人不得自行翻印或仿制。

认证证书内容包括：

a. 获准认证组织名称、地址、社会信用代码、证书注册号（适用时包括总证书号和子证书号）、证书 OID 编号等；

b. 依据的认证标准和认证实施规则等；

c. 获准认证的服务级别（适用时）；

d. 服务覆盖的范围描述，包括服务活动、场所等；

e. 颁证日期/换证日期，有效期说明；

f. 赛西认证的名称、地址与标志；

g. 赛西认证盖章（英文证书由公司总经理签字）；

h. 证书查询方式；

i. 认证证书相关附件（适用时）等。

6.1. 证书的保持

认证证书有效期为 3 年。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。

6.2. 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。

6.3. 认证的暂停、撤销和注销

6.3.1. 暂停

6.3.1.1 获证组织有下列情况之一的，赛西认证经调查核实后将暂停该组织的认证资格：

a. 获证组织因自身原因无法按时接受监督评价、再认证评价，超过规定期限的；

b. 发现获证组织服务持续地或严重地不满足认证要求；

c. 错误使用认证证书、认证标志，未采取纠正措施的；

d. 获证组织被有关执法监管部门责令停业整顿的；

e. 获证组织被地方认证监管部门发现服务活动存在问题，需要暂停证书的；

f. 持有的行政许可证明、资质证书等过期失效，重新提交的申请已被受理但尚未换证的；

g. 获证组织主动请求暂停的；

h. 对于监督评价中提出的不符合项，未按规定时限进行纠正且无合理说明的（或纠正措施未被证实有效的）；

i. 获证后监督评价或服务认证实施规则规定的年限须抽样测评的结果证明服务活动不符合规定的要求，但不需要立即撤销证书的；

j. 由于服务提供者原因，致使不能正常进行抽样的；

k. 获证服务发生与一致性有关内容变更（如服务过程、活动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，服务能力和服务过程的重大变更等，或认证证书所涉及的内容发生变更（如获证组织名称或地址，获证服务范围等），未及时通知赛西认证并办理相关变更手续的；

l. 不承担、履行认证合同约定的责任和义务的；

m. 获证组织发生服务活动重大事故。

6.3.1.2 当做出证书暂停处理后，赛西认证将向获证组织发出“服务认证证书和标志变化通知”，通知获证组织其证书已被暂停。被暂停认证资格期间，获证组织不得以被认证的身份继续宣传其认证状态和使用认证标志。

6.3.1.3 一般情况下，认证资格暂停时间不超过 6 个月。但属于上述 f.情形的暂停期可至相关单位作出许可决定之日。

6.3.1.4 当被暂停认证资格的获证组织在赛西认证规定的期限内采取整改措施，并经验证满足规定的条件后，赛西认证将取消暂停，恢复其认证资格；超过规定时间后将撤销其认证资格，收回证书。暂停期间，经获证组织确认并同意后，可能在暂停期到期前撤销其认证资格。

6.3.1.5 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。

6.3.2. 撤销

6.3.2.1 获证组织有下列情况之一的，赛西认证在获得相关信息并调查核实后将撤销其认证资格。

a. 获证组织被注销或撤销法律地位证明文件的；

b. 被国家质量监督检验检疫总局列入质量信用严重失信企业名单；

c. 拒绝配合认证监管部门实施的监督检查，或者对有关事项的询问和调查提供了虚假材料或信息的；

d. 被暂停认证资格后，未在暂停期限内就存在问题采取相应有效的整改措施的（包括持有的行政许可证明、资质证书等已经过期失效但申请未获批准）；

e. 发现获证组织相关管理体系存在严重违反法律法规要求；

f. 获证组织发生服务活动重大事故，经执法监管部门确认是获证组织违规造成的；

g. 获证组织没有运行服务活动或者因解散、破产、倒闭、经营不善或其它原因已不具备运行条件的；

h. 不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果的，或者赛西认证已要求获证组织纠正但超过 2 个月仍未纠正的；

i. 在认证有效期内，由于认证规则发生变更，获证组织不愿符合新要求的；

j. 其它严重违反与赛西认证正式协议中的有关规定，已造成了严重影响和后果且经查属实的；

k. 获证组织主动要求撤销证书的。

6.3.2.2 当作出撤销获证组织的认证资格后，赛西认证向获证组织发出“服务认证证书和标志变化通知”，通知获证组织其证书已被撤销。被撤销认证资格的获证组织不得继续其所有利用认证资格的活动，并按赛西认证的要求交回所有认证文件。

6.3.3. 暂停、撤销的公示

获证组织的认证证书被暂停或撤销后，赛西认证将在官方网站上进行公示，并按要求上报相关主管部门（CNCA）。

7 认证标志

服务认证标志是证明获证组织的服务符合相应标准与服务认证规则要求的一种象征。

7.1 本领域服务认证准许使用的认证标志样式

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

不允许使用任何形式的变形认证标志。

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。

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。

7.4 赛西认证标志

赛西认证标志是经国家工商行政管理部门登记的受法律保护的标志，由赛西认证随同服务认证证书一起颁发给获证组织合法使用，未经赛西认证允许，获证组织不得将此标志转让给其他组织或个人使用。

赛西认证标志的基本样式如图：



8 证书和标志的使用

认证证书和标志只证明获证组织服务符合申请服务认证标准的要求，不能证明获证组织的产品符合其产品标准或产品安全认证标准的要求，不能证明获证组织的管理体系符合管理体系标准的要求。获证组织可以将认证证书和标志作为符合服务认证标准要求的证明

文件加以应用，但不得将该标志用在产品、产品包装上。也不应以有可能被解释为产品符合要求的方式出现。

获证组织可以将证书和标志用在公开出版物、传播媒介（如互联网、宣传册或广告）上，可在获证服务活动的宣传材料、展示、广告、文件中使用，但不得引起产品或管理体系已通过认证的误解。若认证证书范围缩小，获证组织应随之修改所有相关的宣传资料。

获证组织不得将认证标志使用在与认证范围无关的各类业务及其各类宣传载体上，进行误导宣传。

获证组织在使用认证标志时应接受赛西认证对认证证书和认证标志的正确使用的监督检查。

当获证组织的名称、地址或认证要求发生变化时，应提出申请换发认证证书，赛西认证将重新签发认证证书及附件。

如发现获证组织对认证证书和标志的使用不符合要求、误用或有意错用认证标志、发生对赛西认证认证制度的不正确宣传时，赛西认证将根据其情节的轻重和引起不良影响后果，做出处理，包括：口头或书面警告、要求采取纠正或采取纠正措施、暂停证书、撤销证书资格和公告违规行为及必要的法律措施。

9 申诉、投诉

认证申请方、受审查方以及其他组织和个人均可就与认证活动有关的工作提出书面的申诉、投诉。

申、投诉联系方式见附录 B。

附录 A 证书模板



数据处理活动安全服务认证证书

证书编号：CESI20xxDSMM1xxxxx

OID 编号：1.2.156.1.2. CESI20xxDSMM1xxxxx

兹证明

XX 公司

（统一社会信用代码：xxxxxxxxxxxxxx）

（xxxxxxxxxxxxxxxxxxxxxx）

数据处理活动安全服务能力达到

GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》

★★★★★

X 星 级

认证模式

服务特性测评+服务管理审核+获证后监督

认证规则

CESI-SC-OD11A《数据处理活动安全服务认证规则》

涉及的场所及相关活动：

地址：xxxxxxxxxxxxxx

活动：xxxxxxxxxxxxxxxxxxx

（本证书有效性依据发证机构的定期监督获得保持，证书有效性信息请登录 www.cc.cesi.cn 进行查询）

颁证日期：20xx 年 xx 月 xx 日　　有效期至：20xx 年 xx 月 xx 日

签发人：

北京赛西认证有限责任公司

地　址：北京市东城区安定门东大街一号院 1 号楼 2 层

客服电话：4000719000　　网址：www.cc.cesi.cn

附录 B　CESI 认证业务联系方式

部门	工作内容	联系电话
客户服务部	● 认证申请受理、合同洽谈； ● 认证后服务、认证交费、证书制作、证书领取； ● 申、投诉受理； ● 认证证书、认证标志使用申请受理； ● 变更通报受理	010-64102688 010-64102689 010-64102699
审查二部	● 评价计划安排及实施； ● 认证证书、认证标志使用的监督管理； ● 认证技术支撑	010-64102685
技术委员会	● 认证评定	010-64102692