编号：CESI-SC-OD15

工业和信息化领域数据安全风险评估服务认证规则

2025-8-31 发布　　2025-8-31 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。本规则明确了对工业和信息化领域数据安全风险评估服务机构进行认证的基本原则和要求。

本规则首次发布日期：2023.4.3，实施日期：2023.4.3。

第一次修订（v1.1）日期及内容：2025.8.31，本次换版修订了服务特性测评过程、认证证书模板。

目　录

1 范围

北京赛西认证（CESI）适用于工业和信息化领域数据安全风险评估机构的服务认证。

本规则中认证依据的标准为 《工业和信息化领域数据安全风险评估服务技术规范 V1.0 版》（以下简称“技术规范”）。

技术领域划分：SC12。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期/版本的引用文件，仅所注日期/版本适用于本文件。凡是不注日期/版本的引用文件，其最新版本（包括所有文件修改单）适用于本文件。

GB/T 27065《合格评定产品、过程和服务认证机构要求》

GB/T 27207《合格评定 服务认证模式选择与应用导则》

GB/T 27400《合格评定 服务认证技术通则》

CNAS-SC25：2017《服务认证机构认可方案》

CNAS-GC25《服务认证机构认证业务范围及能力管理实施指南》

3 认证模式

服务管理过程审核+服务特性测评+获证后监督。

4 认证程序

4.1. 认证申请与评审

4.1.1. 申请

申请工业和信息化领域数据安全风险评估服务认证的评估机构（以下简称“评估机构”）应向 CESI 说明关于履行任何相关法律义务的情况，以便 CESI 确定该申请人是否具备申请认证的资格和条件。提交的申请资料如下：

（1） 评估机构已按认证规范要求建立并实施的相关文件：如服务规范、服务提供规范

和服务检验规范等；

（2） 营业执照复印件；

（3） 认证申请书：介绍申请组织的相关详细情况，包括其名称、场所地址、人员、资质、采用的所有影响服务符合性的外包过程。

4.1.2. 申请评审

CESI 在收到评估机构提交的书面申请之日起，在 5 个工作日内对申请材料进行评审。

若评审结论为同意受理，CESI 确认评估机构的位置等内容，与评估机构签订认证合同。若评审结论为不予受理，CESI 以书面形式通知评估机构。

4.2. 审核准备

4.2.1. 组建审核组

CESI 安排具备相关工作经验的审核员、技术专家（必要时）组成审核组。初次认证及再认证审核，审核组原则上应至少由两名审核员组成。

对同一评估机构不能连续 5 年以上（含 5 年）委派同一审核员实施审核。

4.2.2. 下达任务书

CESI 在现场审核前向审核组下达审核任务书，内容包括但不限于：

（1） 评估机构的联系方式；

（2） 认证依据，包括技术规范和其他适用的规范性文件；

（3） 认证范围，包括认证的场所等；

（4） 审核组成员；

（5） 审核的时间要求。

4.2.3. 编制审核计划

审核组应根据任务书要求编制审核计划，并就审核日程安排等提前与评估机构进行沟通。

4.3. 服务管理过程审核

4.3.1. 审核内容

服务管理过程审核至少需确认下列各项：

（1） 对评估机构服务能力的评价，包括对与申请人服务管理系统相关的组织结构、过程、程序、记录及文件的现场评价；

（2） 人员及资源配置与管理；

（3） 服务特性控制及其运行管理；

（4） 用于支持风险评估服务的工具；

（5） 对中断或意外事件的响应和服务补救措施；

（6） 争议的处置管理；

（7） 服务投诉的处理；

（8） 内部审核或评价。

4.3.2. 审核实施

现场审核一般应安排在评估机构的正常经营活动期间；

现场审核首次会议由审核组长主持，确认审核范围、审核目的、审核依据、审核方式、审核日程，宣布审核纪律和注意事项，确定评估机构的审核陪同人员；

审核组对审核中发现的不符合项如实记录，由审核组长汇总，撰写审核报告草案；

现场审核中发现的不符合项，由审核组成员和评估机构负责人签字。如有不能达成共识的问题，审核组应做好记录，经审核组全体成员和评估机构负责人签字；

注：不符合指不能完全满足某个条款的要求。

审核组在末次会议上向评估机构通报现场审核情况，评估机构如对审核发现的问题有不同意见，可作适当解释、说明。

4.3.3. 认证终止

发生以下一种情况时终止认证：

（1） 评估机构申请认证范围内的服务活动被执法部门判定不符合相关法律法规；

（2） 评估机构在约定时间内不能完成不符合项整改或未通过验证。

4.4. 服务特性测评

4.4.1. 服务能力确认或验证

服务特性测评采用能力确认或验证方式。审核组应对服务样本进行服务能力验证，包括对评估技能、专业技术能力以及评估组的管理与协调能力进行确认，以评定评估机构的服务实施能力及服务管理的有效性。数据安全风险评估服务应依据《工业领域数据安全风险评估指南》和/或《电信领域数据安全风险评估指南》，结合客户数据处理活动的范围与类型规范开展。服务需确保评估方法符合标准、覆盖范围全面、过程证据完整可追溯，所识别风险应准确反映实际业务场景，评定结果须包含明确的风险等级和可操作的处置建议，以有效支撑客户安全决策与后续治理工作。

服务能力确认或验证可采用远程或现场的方式。

4.4.2. 服务能力确认或验证样本量计算

服务样本数为评估机构上一年度临时场所（接受风险评估服务的数据处理者）数的平方根，即：y= $\sqrt{X}$ ，

其中：

（1） y 为抽取的服务样本数；

（2） X 为评估机构上一年度临时场所数。

注 1：y 中的 20%（向上取整）为现场样本（现场观察），其余为远程样本（查阅书面项目资料，如：合同、报告、过程记录等）；

注 2：样本数量足够多时，认证证书有效期内，每年访问的场所样本不宜重复；

注 3：现场验证前应通过评估机构征得被评估方同意，评估机构有义务确保抽样量；

注 4：抽样算法参考 CNAS-SC25：2017 服务认证机构认可方案 C.3.11.6。

4.5. 评价报告

CESI 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：

（1） 评价的目的、范围和准则；

（2） 评估机构的基本情况（包括名称、地址等）；

（3） 抽样及样本信息；

（4） 评价结果及其说明；

（5） 与有关认证要求符合性的陈述（包括任何不符合）；

（6） 报告覆盖的时间段；

（7） 形成服务特性测评现场报告(涉及现场验证项目时)。

（8） 结论。

4.6. 复核及认证决定

CESI 根据对评价过程中收集到的有关信息，包括评估机构对不符合项的整改以及评价过程之外获取的任何可作为认证决定依据的信息（如来自行政监管部门、顾客、行业协会的信息等）进行复核，并在 10 个工作日内作出认证决定。

4.7. 监督

4.7.1 监督的内容

CESI 采取适当的方式，对取得认证的服务实施监督，以确认使用标志的服务持续符合技术规范的要求。所要求的监督程序应当包括服务特性测评和服务管理审核等评价活动。

每次服务管理过程审核之间的监督周期不大于 12 个月，两次监督需覆盖认证依据的全部条款。

每个监督周期的服务特性测评内容、抽样按照 4.4.1、4.4.2 要求实施。

每次评价活动完成后编制评价报告。

4.7.2 若发生下述情况之一的，认证机构立即进行现场监督审查：

a）监管部门监督检查中发现严重问题的；

b）获证组织的服务活动出现严重质量问题，如：发生网络安全事故或在网络安全方面有重大投诉，并经查实为获证组织责任的；

c）被检测系统发生严重网络安全事故的；

d）违反法律法规、国家行业监督及媒体曝光等重大问题的。

若发生下述情况之一的，认证机构可适当增加监督频次

a）认证机构有足够理由对获证组织服务与认证要求符合性提出质疑的；

b）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的；

c）存在其他可能影响服务符合性或一致性等特殊情况的。

4.7.3 监督结果的评价

认证机构对获证后监督结论及有关资料/信息进行综合评价，符合认证要求的，可继续保持认证证书；不符合认证要求的，认证机构应根据相应情形作出暂停或者撤销认证证书的处理，并予以公布。

4.8. 再认证

证书到期需延续使用的，评估机构在有效期届满 3 个月内提出认证委托申请，CESI 对其实施再认证。再认证程序与初次认证相同。

5 审核人日

（1） 初次认证和再认证的服务管理过程审核现场工作量不少于 6 人日，总工作量不少于 12 人日；

（2） 监督的服务管理过程审核工作量不少于 3 人日，总工作量不少于 4 人日；

（3） 现场服务特性测评人日=抽取的现场样本数*2 人日；

（4） 远程现场服务特性测评人日=抽取的远程样本数*1 人日。

6 认证的持续改进

认证要求变更时，CESI 将认证要求的变化以公开信息的方式告知评估机构，并对认证要求变更的转换安排做出规定。

7 认证证书

7.1. 认证证书的信息

认证证书至少包含以下信息：

（1） 发证机构及其认证标志；

（2） 证书编号：IITDSRA-CESI-发证日期（YYYY.MM.DD）-流水号（4 位数字）；

（3） 注：再认证时，更新年份保留原流水号。

（4） 证书持有人的名称、地址及其服务提供场所的地址；

（5） 认证范围；

（6） 认证所依据的技术规范；

（7） 发证日期和认证有效期；

（8） 其他需要标注的内容。

7.2. 认证证书的管理

认证证书的有效期为三年。CESI 对评估机构认证证书使用的情况进行有效管理，并在证书换发、暂停、撤销、注销、恢复时采用适当方式公布变更情况。

7.2.1. 认证证书的换发

满足条件时，CESI 为评估机构换发新证：

（1） 评估机构按规定通过再认证审核的；

（2） 评估机构提供工商变更证据证明已变更工商注册信息的；

（3） 评估机构搬迁后已通过监督审核的；

（4） 认证依据更新后，已依据更新后的认证依据通过认证审核的。

7.2.2. 认证证书的暂停

评估机构有包括但不限于下列情形之一的，CESI 暂停其使用认证证书，暂停期限为 3 个月：

（1） 未按期接受监督；

（2） 评估机构未按规定使用认证证书的、认证证书使用不当的；

（3） 评估机构发生违规行为，或行业主管部门抽查不合格等情况，尚不需立即撤销认证证书的；

（4） 顾客对评估机构的服务有投诉，经查实影响评估报告有效性的；

（5） 未按时交纳认证费用的；

（6） 评估机构与 CESI 双方同意暂停认证资格的。

7.2.3. 认证证书的撤销

评估机构有包括但不限于下列情形之一的，CESI 撤销其认证证书。对于被撤销认证证书的评估机构，CESI 在 6 个月内不再受理该评估机构的认证申请：

（1） 未通过监督评价；

（2） 评估机构认证范围内的服务活动被执法部门判定不符合相关法律法规；

（3） 认证证书暂停使用期间，评估机构未采取有效纠正措施的；

（4） 评估机构不再从事证书范围内经营行为的；

（5） 评估机构出现严重违规事故或对相关方重大投诉不采取处理措施的；

（6） 评估机构不接受相应监管部门或 CESI 对其实施的监督的；

（7） 采取不正当手段骗取认证证书的；

（8） 转让认证证书的；

（9） 拒不交纳认证费用的。

7.2.4. 认证证书的注销

评估机构有下列情况之一的，CESI 将注销其认证资格：

（1） 由于认证依据的变更，评估机构达不到新要求且未在限定期限内补充依据的；

（2） 认证有效期届满，评估机构不再提出再次认证申请的；

（3） 评估机构由于经营等原因自动提出放弃认证资格的。

7.2.5. 认证证书的恢复

CESI 对做出暂停认证资格、暂停认证标志使用的评估机构，要求其在规定的时间内完成纠正措施并经 CESI 验证。经验证合格的，恢复其认证资格。

8 与技术争议、投诉和申诉相关的流程及时限要求

CESI 应建立并执行与技术争议、投诉和申诉相关的流程：

（1） 评估机构对于认证环节的技术争议或其他问题可在 10 个工作日内通过电话、电子邮件等方式向 CESI 进行投诉或申诉；

（2） CESI 自收到申诉之日起，应在 1 个月内进行处理，并将处理结果书面通知评估机构；

（3） 评估机构对于处理结果仍存在争议时，可在收到处理结果后 15 个工作日内再次提出争议处理申请；

（4） 二次争议处理结束后，CESI 有权不再响应；

（5） 评估机构认为 CESI 行为严重侵害了自身合法权益的，可以向上级领导机关或国家认监委投诉。

9 认证标志

工业和信息化领域数据安全风险评估服务能力认证标志如下：

获认证的评估机构可在评估报告上使用此标志。证书暂停、撤销、注销时，评估机构不得使用此标志。

标志使用说明：仅在工业和信息化数据安全风险评估服务使用。

10 认证收费

认证费用包括注册费（2000 元）、年金（2000 元）及审核费。注册费为初次申请时一次性收取；年金自申请认证当年开始，每年收取；审核费通过审核人日*人日单价计算，审核人日包含服务管理过程审核+服务能力确认或验证所需人日。

人日单价为 5000 元，不含差旅住宿费。

现场抽样过程中的差旅住宿费由申请认证的评估机构承担。

11 认证责任

CESI 对现场评价结果、认证决定负责。

评估机构应当对认证委托资料的真实性、合法性负责。

附录 A 认证证书样式

工业和信息化领域数据安全风险评估服务认证证书

证书编号：IITDSRA-CESI-20xxmmdd-xxxx

XXXXXXXXXXXXX 公司

统一社会信用代码：xxxxxxxxxxxxxxxxxxx

注册地址：XXXXXXXXXXXXXXXXXXXXXX

认证依据：

工业和信息化领域数据安全风险评估服务技术规范

认证规则：

工业和信息化领域数据安全风险评估服务认证规则

涉及的场所及活动：

运营地址：xxxxxxxxxxxxxxxxxxxxxx

活动：xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

颁证日期：20xx 年 xx 月 xx 日

有效期至：20xx 年 xx 月 xx 日

（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）

（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）

签发人：

北京赛西认证有限责任公司