编号：CESI-SC-OD24

网络安全—安全咨询服务认证规则

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《中华人民共和国网络安全法》、《中华人民共和国认证认可条例》制定，规定了对网络安全服务提供者开展安全咨询服务进行认证的依据、程序及要求。

本规则首次发布日期：2024.8.6，实施日期：2024.8.6。

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

0 引言

本规则依据《中华人民共和国网络安全法》、《中华人民共和国认证认可条例》制定，规定了对网络安全服务提供者开展安全咨询服务进行认证的依据、程序及要求。

网络安全服务认证机构应依据本规则要求编制网络安全服务认证实施细则，并配套本规则共同实施。

1 适用范围

本规则适用于规范网络安全服务认证机构开展网络安全—安全咨询服务认证活动。

认证领域或技术领域划分：SC12。

2 认证依据

GB/T 32914《信息安全技术 网络安全服务能力要求》

上述标准原则上应当执行国家标准化行政主管部门发布的最新版本。

3 认证模式

认证模式为：服务特性测评＋服务管理审核＋获证后监督

4 认证单元划分及认证分级

4.1 认证单元划分

认证单元按照网络安全服务提供者、网络安全服务类别，和不同类别项目等的不同类别项目规模划分。类别划分原则见附表 1，规模划分原则见附表 2.

4.2 认证分级

依据 GB/T 32914 开展的网络安全服务认证，分为一般级和增强

级两个级别。

5 认证程序

5.1 认证委托与受理

5.1.1 认证申请

赛西认证根据法律法规、标准及认证实施的需要在认证申请书中明确认证申请方须提供的基本资料和相关证明文档等。包括但不限于如下资料:

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. 网络安全服务能力认证自评估表（见附表）;
4. 多场所清单（适用时）;
5. 国家级许可资质: （例: 增值电信业务经营许可证）;
6. 其他认证所需相关材料。

认证申请方按要求提供所需资料。

5.1.2 受理

赛西认证负责评审、管理、保存、保密有关资料，并将评审结果告以及是否受理的结论告知认证申请方。

5.2 认证策划

5.2.1 认证方案

赛西认证按认证实施细则的要求制定认证方案，明确认证的目的、范围、依据、方法评估机构及审查组成员及进度安排等。

5.2.2 审查组安排

审查组由1-2名审查员组成。审查组成员应当具备相应领域的专业知识和能力，并与被审查方不存在利益关系。

确定审查组任务分工时，应基于以下方面的考虑:

a）网络安全服务组织的行业特点、规模和运作的复杂程度;

b）网络安全服务场所的数量;

c）网络安全服务类别、评价范围;

d）技术和法规环境;

e）网络安全服务活动的外包情况;

f）与服务活动相关联的风险。

5.2.3 认证时限

赛西认证在认证实施细则中对认证各环节的时限作出明确规定，并确保相关工作按时限要求完成。自正式受理认证委托之日起至出具认证结论之日止，一般不超过90日。

因认证申请方未及时提交资料、不能按计划接受现场审查、未按规定时间递交不符合整改、未及时缴纳费用等原因导致认证时间延长的，不计算在内。因特定领域验证周期等特殊原因导致认证时间延长的，赛西认证与认证申请方协商解决。

5.3 文件审查

赛西认证在收到认证申请方的相关资料后，应按照认证实施细则的要求及时安排文件审查，以判断是否具备现场审查的条件。

对文件审查中发现的不符合，赛西认证提出文件整改要求。认证申请方按照规定的时限完成修改并补充提交必要的文件。

审查组应出具文件审查报告，给出是否进行现场审查的建议及

现场审查中需要关注的事项。

赛西认证制定文件审查要求的具体内容，并在认证实施细则中予以明确。

5.4 现场审查

5.4.1 现场审查计划

现场审查应至少包括服务能力确认或验证和服务管理能力审查（包括服务设计审查、服务管理审查）。当认证申请方的网络安全服务行为的符合性、完整性及准确性不能得到充分证实时，还应辅以服务足迹测评。

审查组应根据文件审查结果制定现场审查计划。现场审查计至少包括目的、范围、依据、日期、审查要求、多场所情况、服务能力确认或验证方案、服务管理能力审查方案等。

现场审查应覆盖申请范围的全部服务认证场所。

5.4.2 服务特性测评

服务特性测评采用服务能力确认或验证方式。

5.4.2.1 服务能力确认或验证样本选取

同一认证单元在抽样时，服务能力确认或验证样本量为受审查方上一年度已签约并完成的网络安全服务项目数量的平方根，计算结果向上取整数。

当样本量不超过 5 个时，应全部进行现场确认或验证。当样本量超过 5 个时，应对至少 30%的样本量进行现场确认或验证，并且数量不少于 5 个，其余样本可采用报告、过程记录验证等远程方式进行确认或验证。

每个样本，应根据项目实施全流程准备方案、过程文档及项目质量等管理记录、项目验收成果等内容。具体见 GB/T 32914-2023 5.3 项目管理章节。

5.4.2.2 服务能力确认或验证实施

认证机构委托具备相应能力的评估机构依据 GB/T 32914 对认证申请方的网络安全服务能力进行确认或验证。并出具《服务能力确认或验证报告》。

评估机构依据 GB/T 32914《信息安全技术 网络安全服务能力要求》等要求选取服务样本、制定服务能力确认或验证的具体内容，并在认证实施细则中予以明确。

5.4.2.3 服务能力确认或验证结论

原则上，在服务能力确认或验证结果为满足的情况下，赛西认证方可安排服务管理能力审查；特殊情况，服务能力确认和服务管理审查可同时进行；但需强调，如服务能力确认或验证结果不满足要求，且受审查方在一个月内无法完成整改，此次认证视为终止。

认证终止的受审查方，需在整改完成 6 个月后方可重新提出认证申请。

5.4.3 服务管理审核

服务管理审核采用服务管理能力审查(包括服务设计审查、服务管理审查)方式。

5.4.3.1 服务管理能力审查实施

赛西认证委派具备能力的服务认证审查组依据 GB/T 32914 的要求对认证申请方附表 3 所列能力进行现场审查。必要时，可聘请技

术专家参加。审查方式包括但不限于:

a）通过现场观察、询问及资料查阅等方式实施审查，以获取认证申请方的环境、策划、支持、运行、绩效评价、改进等相关信息;

b）进入与服务能力评价有关的场所;

c）与服务能力有关的人员进行访谈;

d）通过现场收集网络安全服务案例、过程记录或抽查网络安全服务工作流程等方式实施服务确认或验证，重点关注服务人员能力、风险控制能力、服务工具的安全性、安全咨询记录的可追溯性以及服务流程的一致性等内容。

在获得认证申请方同意后，采用复印、拍摄、录音、笔记等方式保存现场审查记录。

赛西认证制定服务管理能力审查的具体内容，并在相关作业文件中明确。

5.4.3.2 不符合及观察项

现场审查完成后，审查组应根据实际情况向受审查方书面反馈不符合或观察项。认证申请方应在一个月内逐项完成整改，并提供相应的证据材料。审查组根据不符合性质通过书面或现场方式对整改有效性进行验证。

5.4.4 现场审查报告

审查组在完成现场审查后，根据审查实际情况编写现场审查报告。

现场审查报告应至少包括:

a）评价的目的、范围和准则;

b）认证申请方的基本情况（包括名称、地址等）；

c）抽样及样本信息;

d）服务评价结果及其说明;

e）与有关认证要求符合性的陈述（包括任何不符合）；

f）报告覆盖的时间段;

g）现场审查结论。

5.5 复核、认证决定

赛西认证对文件审查结论、现场审查结论以及有关资料/信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书。对存在不合格结论的，认证终止，认证机构不予颁发认证证书。

5.6 申诉与投诉

认证申请方对认证决定结果有异议的，可向赛西认证提出申诉。赛西认证自收到申诉之日起，按照约定的时限处理，并将处理结果书面告知申诉人。

相关方合法权益受到认证机构行为侵害的，可向市场监管部门投诉，并提供证据材料。

6 获证后监督

6.1 监督的方式和频次

认证申请方在认证有效期内，采用合理的频次对获得认证的网络安全服务进行现场监督审查，确保其持续符合认证要求，监督周期不大于 12 个月。

若发生下述情况之一的，赛西认证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）赛西认证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。

6.2 监督的内容

监督应至少包括服务能力确认或验证和服务管理能力审查。监督内容为认证依据标准规定的部分条款，证书有效期内的监督应覆盖全部条款。

6.3 监督结果的评价

赛西认证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。

7 认证证书和认证标志

7.1 认证证书

7.1.1 认证证书的保持

认证证书有效期为 3 年。在有效期内，证书有效性通过认证机构的获证后监督保持。

证书到期需延续使用的，认证申请方应当在有效期届满前 6 个月内提出认证委托，赛西认证对其实施再认证，再认证程序应与初次认证相同。

7.1.2 认证证书的变更

认证证书有效期内，若获得认证的网络安全服务提供者的名称、注册地址、办公地址、组织架构、高层管理人员、管理制度或认证范围等发生变化时，认证申请方应当向认证机构提出变更委托。

赛西认证根据变更的内容，对变更委托资料进行评价，确定是否可以批准变更。如获得认证的网络安全服务提供者发生的变更可能影响服务符合性或一致性，赛西认证在批准变更前进行现场审查。

赛西认证受控管理证书的变更。

7.1.3 认证证书的暂停、恢复、注销和撤销

认证证书的使用应当符合国家认监委有关认证证书管理的要求。当认证申请方违反认证有关规定，或获得认证的网络安全服务不再符合认证要求时，赛西认证会及时对认证证书予以暂停直至撤销，并将处理结果进行公布。认证申请方在认证证书有效期内可向认证机构申请暂停、注销其持有的认证证书。

认证证书暂停期间，注销、撤销和过期失效后，获证组织不得使用认证证书和认证标志。

认证证书暂停期间，认证申请方如果需要恢复认证证书，应在规定的暂停期限内向认证机构提出恢复申请，赛西认证按认证实施细则的要求进行恢复处理。

认证机构应制定认证证书暂停、恢复、注销和撤销的具体要求，

并在认证实施细则中予以明确。

7.2 认证证书的使用

在认证证书有效期内，获得认证的网络安全服务提供者应当按照有关规定在广告等宣传中正确使用认证证书，不得对公众产生误导。

7.3 认证标志

本规则不使用认证标志。

附表 1：项目类别划分原则

	安全咨询	安全运维	安全咨询
服务内容	如：渗透测试、系统安全检测、网络安全风险评估、数据安全风险评估、个人信息保护影响评估、安全审计等	如：驻场安全运维、网络安全监测与态势感知、安全托管运营、重保现场值守、安全应急响应支持等	如：安全设计与开发咨询、安全规划与集成咨询、安全管理体系建设咨询、安全培训等

附表 2：项目规模划分原则

合同额	安全咨询	安全运维	安全咨询
小型项目	10 万以内	20 万以内	10 万以内
中型项目	50 万以内	100 万以内	50 万以内
大型项目	50 万以上	100 万以上	50 万以上

附表 3：服务管理审查

级别	GB/T 32914：2023
一般	5.2 组织管理； 5.4 供应链管理； 5.8 法律保障； 5.10 服务可持续性

增强	6.2 组织管理 6.3 供应链管理 6.7 服务可连续性

附录 A 认证证书样式

网络安全—安全咨询服务认证证书

证书编号：CESIxxCSSC2xxxxRx

OID 编号：1.2.156.1.2. CESIxxCSSC2xxxxRx

兹证明

XXXXXXXXXXXX 公司

（统一社会信用代码：XXXXXXXXXXXXXX）

（XXXXXXXXXXXXXXXXXX）

网络安全—安全咨询达到

GB/T 32914-2023

《信息安全技术 网络安全服务能力要求》

XX 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-OD24《网络安全—安全咨询服务认证规则》

涉及的场所及相关活动：

地址：xxxxxxxxxxxxxxxxxx

活动：xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

（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）

（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）

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

签发人：

发证机构：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