附件 2

数据安全风险评估服务认证规则

（国家（　））

2026-8-20

中央网信办（国家网信办）数据与技术保障中心

1

本规则依据《数据安全法》《网络数据安全管理条例》《中华人民共和国认证认可条例》《网络数据安全风险评估办法》制定。本规则明确了对数据安全风险评估专业机构提供的数据安全风险评估服务进行认证的基本原则和要求。

本规则适用于面向数据安全风险评估专业机构的数据安全风险评估服务认证。

2

GB/T 45389-2025《数据安全技术 数据安全评估机构能力要求》

GB/T 45577-2025《数据安全技术 数据安全风险评估方法》

3

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）服务足迹测评，简称模式 F;

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:

1）服务能力确认或验证，简称模式 G;

2）服务管理审核，简称模式 I。

初次认证、再认证: 服务管理审核（模式 I）+服务能力验证或确认（模式 G）+服务足迹测评（模式 F），服务特性测评至少覆盖一次完整的服务活动/过程。

获证后监督: 一个监督周期内应包括服务管理审核（模式 I）、服务足迹测评（模式 F）、服务能力验证或确认（模式 G）。

4

单一领域: 数据安全风险评估。SC12 电信服务; 信息检索和提供

服务。

5

5.1 认证申请

认证申请组织在申请认证时，应至少提交以下资料:

1) 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、资质等;

2) 在中华人民共和国境内注册证明材料;

3) 法定代表人、主要负责人为中华人民共和国境内的中国公民证明材料，以及无犯罪记录证明;

4) 对认证要求符合性的自评价结果及相关证明文档;

5) 与申请认证服务范围相适应的数据安全风险评估人员配置及能力证明材料;

6) 数据安全风险评估服务标准、服务工作手册、服务规范性文件等管理文件;

7) 中国合格评定国家认可委员会颁发的实验室认可证书或检验机构认可证书，且证书处于有效状态，证书认可的能力范围含信息安全、网络安全、数据安全等检验检测相关内容;

8) 其他需要的文件。

申请组织应对所提交材料的真实性、完整性、有效性负责。

5.2 申请受审与认证合同

[illegible]申请组织提交的[illegible]面申请之[illegible]起，认证机构应

日

本不宜重复；场所的抽样数量计算结果向上取整数。

5.3.2.2 样本抽样

初次认证时，申请组织提供符合要求的服务特性测评样本量不少于2个；监督及再认证时，认证机构对获证组织抽样时，服务特性测评样本量为获证组织上一年度已完成的数据安全风险评估服务项目数量平方根，即：$Y=\sqrt{X}$，计算结果向上取整数，样本量最多不超过5个。

1) Y为抽取的服务项目样本数；

2) X为获证组织上一年度已完成的数据安全风险评估服务项目数。

注：抽样时，应保证样本的多样性、代表性。

5.3.3 审查时间

审查人日数（1人日为8小时）如下所示：

1) 初次认证和再认证的现场管理审核人日数不少于5人日，现场服务特性测评人日数（服务能力确认或验证、服务足迹测评）不少于5人日；

2) 监督的现场管理审核人日数不少于2人日，现场服务特性测评人日数不少于3人日；

3) 多场所时，每个场所的服务管理审核增加0.5人日；

4) 现场服务特性测评人日≥现场服务管理审核人日。

5.3.4 组建审查组

认证机构安排具备相关工作经验的审查员、技术专家（必要时）组成审查组。审查组应至少包括1名审查员，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SC12专业服务认证审查员注册资格。服务特性测评应由具有SC12专业审查员实施。

实习审查员、技术专家不得独立开展审查活动。

5.4 评价

5.4.1 下达任务书

认证机构在现场评价前向审查组下达评价任务书，评价内容包括但不限于:

1) 认证申请组织的联系方式;

2) 评价依据，包括技术规范和其他适用的规范性文件;

3) 评价范围，包括评价的场所等;

4) 审查组成员;

5) 审查的时间要求。

审查组根据任务安排，负责服务管理审核、服务能力确认或验证、服务足迹测评之一或其组合的评价工作。

5.4.2 编制评价计划

审查组应根据任务书要求编制评价计划，并就评价日程安排等提前与认证申请组织进行沟通。服务管理审核形成审核计划，服务特性测评形成测评计划。

认证评价应安排在认证范围覆盖的服务活动正常运行时进行。审查组在编制评价计划时，应当充分考虑服务正常运行时段和风险时段，确保服务特性测评时能捕捉到服务最真实的运行状态。

5.4.3 现场评价

审查组对认证申请组织实施服务的场所进行现场评价。

1) 召开首次会议，认证申请组织关键岗位人员（最高管理者或其书面授权的其他高级管理层成员，及服务能力体系覆盖范围部门领导）应参加会议。审查组在首次会议上向认证申请组织说明评价目的、评价依据、评价覆盖范围和评价方法、明确受限制区域，确认认证申请组织的评价计划，同时将可能引起评价中止的条件告知认证申请组织。如双方有不同意见，应协商解决。认证申请组织需对服务运行与管理、认证

准备等情况进行介绍。

2)审查组根据评价计划及现场评价记录单，采用沟通访谈、查阅文件记录、现场观察等方法，对认证申请组织的服务管理过程进行审查，取得客观证据，并记录审查结果。

3)在审查期间，认证申请组织应予协助、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) 允许观察员（如行业监督部门委派）参与。

4)现场评价结束前，审查组应与认证申请组织负责人（或其授权代表）进行交流沟通，表明审查组现场评价的意见。召开末次会议，认证申请组织关键岗位人员（最高管理者或其书面授权的其他高级管理层成员，及服务能力体系覆盖范围部门领导）应参加会议。审查组表明现场评价的结论。

5)发生下列情况的，审查组应向认证机构报告后终止审核：a）认证申请组织对审查活动不予配合，审查活动无法进行；b）认证申请组织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；c）认证申请组织实际情况与申请材料有重大不一致；d）其他导致审查程序无法完成的情况。

5.4.4 服务特性测评

5.4.4.1 服务能力确认或验证

服务特性要求:

1)评估过程按照 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》实施;

2)评估报告内容按照 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》编制;

3)服务提供和交付过程中，评估人员具备开展数据安全风险评估所需资质，客观公正、态度友好;

4)按时出具评估报告。

评价方法如下:

1)服务样本数：见 5.3.2 计算的样本量;

2)现场观察认证申请组织的服务能力，包括对评估流程、专业技术能力以及服务态度进行验证，以评价认证申请组织的服务效果;

3)依据 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》，对第 6-10 章进行评价;

4)计算评估报告出具时间;

5)查看主要评估人员的资质。

判定规则：测评结论分为合格、不合格。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，评估报告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。应按照合同约定的服务周期及时完成评估报告。服务人员态度良好，交流畅通。主要评估人员均具有资质。满足以上要求，测评结论合格。

5.4.4.2 服务足迹测评

服务足迹测评依据 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》。

审查组查阅认证申请组织近一年已完成的真实项目服务记录，评价:

1)评估过程按照 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》实施;

2)评估报告内容按照 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》编制;

3)服务提供和交付过程中，评估人员具备开展数据安全风险评估所需资质，客观公正;

4)按时出具评估报告。

评价方法如下:

1)服务样本数: 见 5.3.2 计算的样本量;

2)依据 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》，对第 6-10 章进行服务记录评价;

3)计算评估报告出具时间;

4)查看主要评估人员的资质。

判定规则: 测评结论分为合格、不合格。服务评估方法符合标准、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。应按照合同约定的服务周期及时完成评估报告。主要评估人员均具有资质。满足以上要求，测评结论合格。

5.4.5 服务管理审核

初次认证/再认证，服务管理审核依据 GB/T 45389-2025《数据安全技术 数据安全评估机构能力要求》全条款开展，以确定服务管理能力是否符合要求。多场所时，样本场所根据管理职责、复杂程度，增加适当条款。

服务管理过程审核至少需包括下列各项:

1)对认证申请组织服务能力的审核，包括对与认证申请组织评估服

务管理过程相关的组织结构、过程、程序、记录及文件的现场审查;

2)人员及资源配置与管理;

3)用于支持服务的设施设备、服务工具、信息技术及相应的环境条件;

4)服务特性控制及其运行管理;

5)对中断或意外事件的响应和服务补救措施;

6)服务承诺和顾客服务;

7)服务投诉、争议的处置管理;

8)内部审核;

9)持续改进。

根据服务管理过程审核结果，分为通过、基本通过、不通过。服务管理过程未发现问题，结论是通过；服务管理过程出现偶发问题，但不影响认证申请组织的管理质量，结论是基本通过；服务管理过程出现系统性问题，或认证申请组织的管理体系运行已失效，结论是不通过。

5.4.6 不符合事项的处置

1)服务管理审核结论为“基本通过”或“通过”时，服务管理审核中发现的任何可能被判定为不符合的问题，以不符合项报告的形式告知申请组织，并应在规定的期限内采取措施;

2)服务特性测评中发现的任何可能被判定为不符合的问题，以测评结果报告和其他适当的方式告知申请组织，需要时，重新取样并再次实施服务特性测评，或终止认证。

认证申请组织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，上报认证机构。

5.4.7 评价报告

认证机构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) 申请组织的基本情况（包括名称、地址等）