数据安全风险评估服务认证规则

编号：CCRC-DSC-DSRA-001:2026

B/0

中国网络安全审查认证和市场监管大数据中心 发布

2026-7-24 发布 2026-8-20 实施

1适用范围

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认证依据

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认证模式

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领域划分

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认证程序

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申请评审与认证合同

认证机构在收到认证申请组织提交的书面申请之日起，认证机构应对申请资料进行评审，确认申请条件满足后受理。申请组织应同时满足以下条件：

1)具有覆盖服务范围的法律地位证明材料；

2)提供完整的申请材料；

3)当前未被行政监管部门责令停产停业整顿；

4)当前未被列入“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。

且认证机构确保：

1)认证过程所需的客户信息是充分的；

2)认证机构和认证申请组织之间任何已知的理解上的分歧已经得到解决,包括在相关标准或规范性文件方面达成一致；

3)实施所有评价活动的方法是可行的；

4)认证机构有能力并能够实施认证活动。

认证机构对申请资料进行评审后作出受理或不予受理的决定，若评审结论为不予受理，认证机构以书面形式通知认证申请组织。

通过申请评审后，认证机构应与认证申请组织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、违约条款以及认证申请组织和认证机构的责任。

若决定受理，认证机构根据认证申请资料确定评价方案，并通知认证申请组织。

5.3评价策划

5.3.1总则

认证机构应对服务管理审核、服务特性测评等活动进行策划。

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》。

服务特性测评依据 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》以及相关要求。

5.3.2抽样

5.3.2.1 多场所抽样

应对认证申请组织申请范围内的所有场所进行现场评价。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。组织的所有场所同属一个服务系统，各场所实施的服务流程和执行的服务标准/规范相同，不会因场所不同而影响服务提供和交付的结果；且这些活动都处于该申请组织同一管理体系控制下，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。抽样包括但不限于随机抽样、分层抽样等。抽样方案还应考虑下列特殊情形：

1）认证申请组织管理体系的中心职能不参与抽样；

2）对于不同管理模式的多场所，应分层抽样；

3）样本需覆盖对服务内容、流程有特别要求的；

4）选取样本还宜考虑人员规模、地域差异、语言、内外部监督结果或以往的服务评价结果、投诉情况以及上次服务评价或服务认证后的变化。

样本计算，抽取场所数为认证申请组织常设场所数的平方根，即：$y=n\sqrt{x}$，

1)y 为抽取的服务场所样本数；

2)x 为认证申请组织常设场所数；

3)n 为抽样系数，初次认证宜为[1.8,2]，监督宜为[1.1,1.2]，再认证宜为[1.5,1.6]。

抽取的场所样本中，由认证机构随机抽取至少 25%的场所样本。

根据抽取样本场所的管理职责、人员规模、复杂程度，认证机构安排服务管理能力审核。认证机构应对随机抽取的场所安排服务能力验证或确认，其余抽样场所应安排服务足迹测评。

注 1：样本数量足够多时，认证证书有效期内，每年监督的场所样本不宜重复；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。审查组应至少包括 1 名具有 SC12 专业审查员或技术专家。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）；

3)审查组组成，审查时间；

4)报告覆盖的时间段；

5)抽样及样本信息；

6)与本次评价内容有关的陈述（包括任何不符合）；

7)评价结果及其说明；

8)（适用时）不符合项整改情况；

9)结论；

10)其他信息。

5.5认证复核

认证机构在作出认证决定前，应对认证审查资料进行复核。复核内容至少包括：

1)申请组织提交的申请资料及相关证明材料；

2)文件评审结果、现场审查结果（服务管理审核结果、服务特性测评结果等）及相关记录；

3)审查/测评活动对申请认证范围、服务场所及关键服务过程的覆盖情况；

4)认证依据、认证模式及认证结果判定要求的适用情况；

5)评价报告及处置情况（如有）；

6)与认证决定相关的其他信息。

5.6认证决定

认证申请组织应符合下列条件：

1)与认证机构签署了正式服务认证合同，满足申请方条件（见 5.2）；

2)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；

3)认证评价程序符合规定要求，认证资料完整、手续齐全；

4)对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；

5)未发现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。

对服务管理审核结论“基本通过”以上，且服务特性测评结果合格的，颁发认证证书；对服务管理审核结论“不通过”，或服务特性测评结果不合格的，不予授证，并以书面形式通知认证申请组织。

涉及更新、扩大认证范围的条件、不予认证决定条件见6.3。

5.7获证后监督

5.7.1监督的频次和要求

认证机构在认证证书有效期内，通过认证评价对获证组织进行持续监督，初次认证后的第一次监督审查在颁发证书日期起12个月内进行，年度监督审核至少每个日历年进行一次（再认证除外），且两次监督评价时间间隔不得超过12个月。超过期限而未能实施监督的，应给予暂停。

若发生下述情况之一的，认证机构可适当增加监督频次。

1)监管部门监督检查中发现严重问题的；

2)获证组织的服务活动出现严重质量问题，如：评估服务客户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的；

3)出现违反法律法规、国家行业监督及媒体曝光等重大问题的；

4)认证机构已获取足够信息对获证组织服务与认证要求符合性提出质疑的。

多场所抽样，监督人日计算方法，见5.3.2、5.3.3。

5.7.2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)数据安全风险评估服务项目是否有效运行；

3)数据安全风险评估服务的变更不影响其满足服务特性要求；

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

5)数据安全风险评估服务管理过程是否持续开展；

6)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；

7)是否及时接受和处理投诉。

服务管理审核采用条款抽样的方式开展，两次监督需覆盖“GB/T 45389-2025”全部条款。多场所时，根据抽样场所的管理职责、人员规模、复杂程度，安排适当服务管理审核条款。

1 个认证周期内监督服务特性测评内容覆盖完整的服务活动/过程。抽样按照5.3.2 要求实施。

5.7.3获证后监督结果决定

认证机构对证后监督评价报告和其他相关资料信息进行综合评价，作出认证决定。若服务管理审核结论为“基本通过”或“通过”、服务特性测评结论为“合格”，可继续保持认证证书；若服务管理审核结论为“不通过”，或服务特性测评结论为“不合格”，认证机构根据相应情形作出暂停直至撤销认证证书的处理，并予以公布。

5.8再认证

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

再认证过程、认证决定与初次认证要求一致，再认证多场所抽样、人日计算方式见 5.3.2、5.3.3。

5.9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）。

6认证证书

6.1认证证书的信息

认证证书至少包含以下信息：

1)认证机构的名称及其机构标识；

2)证书编号；

3)证书持有人名称、地址（包括注册地址及具体的服务运营场所/服务场所）；

4)认证范围；

5)认证依据的标准、技术要求；

6)发证日期和认证有效期；

7)认证证书的查询途径；

8)其他需要标注的内容。

认证证书有效性查询：通过国家认监委网站 www.cnca.gov.cn，以及各认证机构采取的公开方式查询。

6.2证书有效期

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。

6.3认证的变更

6.3.1 认证范围变更

认证证书有效期内，获证组织申请认证范围变更（如服务场所扩大或缩小、搬迁等）时，认证机构应对变更申请进行评审。根据变更内容，认证机构开展对获证组织的评价、复核和评定。获证组织同时满足下列条件的，认证机构可作出换发证书的决定，证书原有效期不变。

1)更新后的认证范围属于本规则规定的服务认证范围；

2)获证组织提交的更新资料真实、完整、有效；

3)更新后的证书信息与获证组织实际提供的服务活动一致，且符合本规则规定的认证依据要求；

4)认证机构已根据更新情况实施必要的评价活动，评价结果满足本规则要求；

5)证书信息更新不影响获证组织认证持续有效性；

6)获证组织已按照认证合同约定履行相关义务。

当获证组织不满足要求时，认证机构应做出认证范围不予变更的结论，并书面通知获证组织。

6.3.2 获证组织其他变更

认证证书有效期内，获证组织名称、管理体系、人员/设备设施等发生重大变化时，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，对变更申请进行评审。认证机构根据变更情况，开展对获证组织的评价、复核和评定，当获证组织满足要求后，认证机构换发认证证书，证书原有效期不变。当获证组织不满足要求，应对证书进行暂停，并按照暂停流程处置。

6.3.3 认证要求变更

当认证机构提出对获证组织产生影响的新的或修订的认证要求时，如认证依据标准、认证模式等发生变化，认证机构应通知获证组织实施认证变更。认证机构对获证组织开展评价、复核和评定，当获证组织满足要求后，认证机构换发认证证书，证书原有效期不变。当获证组织不满足要求，应对证书进行暂停，并按照暂停流程处置。

6.4认证的暂停、恢复、撤销和注销

6.4.1认证证书的暂停

获证组织发生下列情形之一（包括但不限于）的，认证机构暂停认证证书：

1)获证组织未按规定使用认证证书、认证证书使用不当的；

2)获证组织发生违规行为（如违反《网络数据安全风险评估办法》），尚不需立即撤销认证证书的；

3)顾客对获证组织的服务有投诉，经查实影响评估报告有效性的；

4)获证组织与认证机构双方同意暂停认证资格的；

5)被行政监管部门责令停产停业整顿；

6)其他需要暂停的情形。

认证证书暂停期限最长为90天。认证机构采用适当方式对外公布被暂停获证组织认证证书，通知获证组织暂停认证证书和认证标志的使用。

6.4.2认证证书的恢复

获证组织在规定的时间内采取纠正措施完成整改，向认证机构提出恢复申请。经认证机构验证通过的，恢复其认证资格。认证机构对外更新认证证书信息。

6.4.3认证证书的撤销

获证组织出现下列情形之一（包括但不限于）的，认证机构撤销其认证证书：

1)获证组织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)认证证书暂停使用期间，获证组织未采取有效纠正措施的；

3)获证组织的经营范围变更后，评估活动不在经营范围内的；

4)获证组织出现违规行为（如违反《网络数据安全风险评估办法》）且造成重大不良影响的；

5)被列入“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的；

6)获证组织对相关方重大投诉不采取处理措施的；

7)获证组织不接受相应监管部门或认证机构对其实施的监督的；

8)采取不正当手段骗取认证证书的；

9)转让认证证书的；

10)其他撤销的情形。

认证机构采用适当方式对外公布被撤销获证组织认证证书，并收回证书，取消其认证标志使用资格。

对于被撤销认证证书的获证组织，认证机构在 12 个月内不再受理该组织的认证申请。

6.4.4认证证书的注销

获证组织有下列情况之一的，认证机构将注销其认证资格：

1)由于认证依据的变更，获证组织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，获证组织不再提出再次认证申请的；

3)获证组织由于经营等原因自动提出放弃认证资格的。

认证机构采用适当方式对外公布被注销获证组织认证证书，并收回证书，取消其认证标志使用资格。

7认证标志

1)“CCRC”代表认证机构识别信息。

2)规格：标志图案的尺寸长宽比例 1:1，允许线性比例缩放。不允许变形使用认证标志。

3)颜色：应使用基本颜色或单一黑色。

在认证证书有效期内，获证组织应当按照有关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。获证组织可在评估报告上使用认证标志。

8争议、投诉和申诉

认证机构应建立并执行争议、投诉和申诉相关的流程：

1)申请组织/获证组织对于认证环节的争议或其他问题可在10个工作日内通过电话、电子邮件等方式向认证机构进行投诉或申诉；

2)认证机构自收到申诉之日起，应当在1个月内进行处理，并将处理结果书面通知申请组织/获证组织；

3)申请组织/获证组织对于处理结果仍存在争议的，可在收到处理结果后10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，认证机构有权不再受理；

5)申请组织/获证组织认为认证机构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收费

收费标准见认证机构公开文件。

10认证责任

认证机构对现场评价结果、认证决定负责。

申请组织/获证组织应当对认证委托资料的真实性、合法性负责。