信息技术服务商安全交付能力服务认证

合作检验评估机构管理规则（试行）

2026 年 8 月 31 日发布 2026 年 8 月 31 日实施

信息技术服务商安全交付能力服务认证
合作检验评估机构管理规则（试行）

1 范围

本文件规定了信息技术服务商安全交付能力服务认证合作的检验评估机构的能力要求、评定流程以及对评估机构的控制。

本文件适用于信息技术服务商安全交付能力服务认证合作的检验评估机构的评价、决定与控制。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 27020—2016 合格评定 各类检验机构的运作要求

GB/T 27025—2019 检测和校准实验室能力的通用要求

CSP-S01-002：2025 信息技术服务商安全交付能力服务认证规则

CTS CSP-J019：2025 信息技术服务商安全交付服务能力要求

3 术语和定义

3.1 检验评估活动

根据认证规则和技术规范，对认证申请方开展的增强技术测试。

注：简称“评估活动”。

3.2 检验评估机构

与认证中心合作，从事评估活动，并向认证中心提供评估结果的第三方机构。

注：简称“评估机构”。

3.3 监督

在合作有效期内，为验证评估机构是否持续符合要求而开展的评价。

4 能力要求

4.1 基本条件

评估机构应具备以下基本条件：

a) 在中华人民共和国境内注册成立的法律实体，或者为某个法律实体的明确部分，该实体应当经所在法人单位授权并对其全部评估活动承担法律责任；

b) 由中国公民、法人投资或者国家投资成立，注册资金不低于人民币 1000 万元；

c) 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，且无犯罪记录；

d) 未被列入失信被执行人、重大税收违法案件当事人名单和政府采购严重违法失信行为记录名单等，以及其他可能影响评估机构能力和信誉的负面清单；

e) 具有中国合格评定国家认可委员会颁发的检验机构认可证书或实验室认可证书，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、人工智能安全等检验检测相关内容；

f) 具有关键信息基础设施运营者或保护工作部门出具的书面推荐材料。

4.2 公正性、独立性与保密要求

评估机构的公正性、独立性与保密应符合以下要求：

a) 严格执行有关法律法规、标准规范，开展客观、公正的评估活动，并以公开方式对其遵守法定要求、独立公正从业、履行社会责任、严守诚实信用等情况进行自我承诺；

b) 对其评估活动的公正性负责，不受可能来自商业、财务或其他方面的压力而

影响公正性；

c) 独立于其出具的评估数据、结果所涉及的利益相关方，不受任何可能干扰其技术判断的因素影响，保证评估数据、结果公正准确、可追溯；

d) 不从事面向关键信息基础设施运营者或保护工作部门的软硬件开发和运营运维服务，由国家机关授权或评估机构内部独立开展的除外；

e) 不向评估对象推荐、指定产品或服务；

f) 对其在评估活动中所知悉的国家秘密、商业秘密负有保密义务，并制定实施相应的保密措施，涉及国家秘密的参照国家保密相关规定。

4.3 人员要求

评估机构的授权签字人、专业分析人员、技术测试人员（以下统称评估人员）应符合以下要求：

a) 评估人员与评估机构建立正式劳动关系，且符合《中华人民共和国劳动法》《中华人民共和国劳动合同法》的有关规定；

b) 评估人员具有网络安全相关领域 3 年及以上的工作经验，并具备评估活动所需的专业知识和技能；

c) 授权签字人应具有高级专业技术职称或同等能力；

注：同等能力是指博士研究生毕业，从事相关专业评估活动 1 年及以上；硕士研究生毕业，从事相关专业评估活动 3 年及以上；大学本科毕业，从事相关专业评估活动 5 年及以上。

d) 评估人员在正式上岗前，参加认证中心组织的专项培训并通过考核；

e) 评估机构的评估人员不应少于 15 人。

4.4 场所和环境要求

评估机构自身场所和环境应符合以下要求：

a) 评估机构实际工作场所与中国合格评定国家认可委员会颁发的检验机构/实

验室认可证书的场所地址一致；

b) 评估机构具有固定的工作场所，场所环境、安全条件、功能布局等满足评估活动的要求。

4.5 设备和工具要求

评估机构用于评估活动的设备和工具应符合以下要求：

a) 配备的评估设备和工具满足评估工作需要（类型见附件 1）；

b) 评估机构使用租用、借用的设备和工具的，应当有合法的租用、借用合同，租用、借用期限不少于 1 年，并对租用、借用的设备和工具具有完全的使用权、支配权；

c) 设备和工具的功能仅限于其声明的功能，不应包含后门、隐蔽通道及其他恶意功能，由研制生产单位出具证明或权威机构提供检测报告；

d) 确保所有设备和工具的合法版权且授权在有效期内，运行状态良好，对于开源工具，需确保其合法使用权利，并评估和保障其安全性；

e) 持续关注设备、工具及其组件的安全漏洞公告和相关信息，及时更新维护，并在投入使用前对其安全性进行验证确认，在使用期间定期核查、持续更新；

f) 具备设备和工具管理制度，明确其登记标识、操作使用、存放保管、维修维护等方面的要求。

4.6 管理体系要求

评估机构的管理体系应符合以下要求：

a) 评估机构依据 GB/T 27020—2016 或 GB/T 27025—2019 中相关要求，建立与自身实际情况相适应的管理体系；

b) 管理体系以恰当的形式体现，包括但不限于质量手册、程序文件、作业指导书等；

c) 评估机构在管理体系中明确保护评估数据完整性、安全性和不可伪造篡改的内容，并采取密码技术、数据防泄漏等措施保护评估数据安全；

d) 评估机构开展评估活动的原始记录信息充分、清晰、完整，记录和报告保存期限不少于 6 年；

e) 评估机构应建立并维护自身网络安全能力，以识别、防范和应对评估活动相关的网络安全风险。

5 评定流程

5.1 总则

认证中心依据本文件 4 能力要求的所有条款要求，对申请机构的能力进行评价。

5.2 文件审查

认证中心对申请机构提交的申请书（附件 2）及其他资料的合规性、完整性、有效性进行形式审查。

5.3 专家评审

对通过文件审查的申请机构，认证中心组织专家进行评审，形成评审意见。

5.3 现场评价

5.3.1 对通过专家评审的申请机构，认证中心开展现场评价，现场评价包括访谈相关人员，查看环境、设施、工具，审阅体系文件、程序文件和项目文档等。

5.3.2 认证中心策划评价方案，组建成立评价组。评价组成员应熟悉《信息技术服务商安全交付能力服务认证规则》《信息技术服务商安全交付服务能力要求》。评价组长出具现场评价报告，并给出评价结论。

5.4 决定

对通过现场评价的申请机构，认证中心按照程序作出是否建立合作的决定。

5.5 签订合作协议和建立机构名录

认证中心与评估机构签署合作协议，并于 5 个工作日内发布评估机构名录。

6 对评估机构的控制

6.1 投诉和申诉处理

认证中心对与评估机构相关的投诉或申诉进行记录、调查与处理，并将处理结果及时通知投诉人或申诉人。

6.2 监督

6.2.1 定期监督

认证中心按年度对评估机构实施监督，依据业务开展情况对本文件 4 能力要求的所有条款要求进行抽样验证，对观察项进行跟踪验证。

6.2.2 不定期监督

认证中心根据与评估机构有关的投诉情况，有针对性地对其进行跟踪和验证。

6.3 合作的保持

认证中心根据监督情况作出是否保持合作的决定。

6.4 合作的暂停与终止

6.4.1 合作暂停

评估机构出现下列任一情形时，认证中心可暂停与评估机构的合作：

a) 提交申请评估机构的资质失效的；

b) 拒绝认证中心监督或投诉处理的；

c) 监督不合格的；

d) 评估报告未采用认证中心规定模板或存在明显错误，造成认证业务停滞。

评估机构应在暂停后三个月内完成整改并提交恢复合作申请，认证中心在收到评估机构恢复申请后的 15 个工作日内，作出是否恢复合作的决定。

在暂停合作期间，认证中心停止采信评估结果并发布公告，评估机构应停止开展评估活动，合作暂停的时间计入合作有效期，由此造成的损失由评估机构自行承担。

6.4.2 合作终止

评估机构出现下列任一情形时，认证中心可终止与评估机构的合作：

a) 违反国家有关规定并受到处罚的；

b) 未实质性开展评估活动，伪造、篡改评估数据，出具虚假评估报告的；

c) 泄露评估对象的技术资料、评估数据和评估结果的；

d) 合作暂停后，未在规定期限内完成整改并通过验证；

e) 其他严重违反认证中心要求的行为。

合作终止后，评估机构应停止开展任何评估活动，认证中心于 5 个工作日内更新评估机构名录。

附件 1

设备和工具类型

设备和工具是信息技术服务商安全交付能力增强技术测试的辅助手段，根据任务场景、作用原理的不同，下表给出了评估活动中可能需要的设备和工具类型示例。

序号	工具类型	主要功能
1	软件成分分析工具	1.支持源代码、二进制制品或依赖库静态扫描； 2.支持自动识别软件组成成分（开源组件、许可证）； 3.支持开源组件漏洞风险、许可证合规风险及配置风险检测； 4.支持 Java、C、Python、Go、JavaScript 等主流编程语言生态，依据 GB/T 47020-2026 标准生成并输出 SBOM。
2	有效性验证工具	通过自动化攻击模拟技术，对网络安全防护和检测能力进行有效性验证评估。支持验证的能力包括但不限于： 1、边界安全防护能力； 2、主机与终端安全防护能力； 3、流量安全防护能力； 4、勒索攻击防护能力； 5、邮件钓鱼攻击防护能力。
3	代码审计工具	在不运行代码的情况下对源代码进行安全缺陷扫描。 1、支持 C/C++、Java、Python、Go 等主流开发语言源码扫描； 2、覆盖 CWE Top 25 代码级高危缺陷及 OWASP Top 10 应用漏洞检测； 3、支持自动生成可复现的漏洞 POC，直接用于漏洞验证； 4、支持对 Jar 包、War 包进行分析。 注：推荐优先采用代码审计智能体。
4	漏洞扫描工具	1、支持对网络产品、物联网设备、主机与终端、应用系统在内的内外网资产进行测绘； 2、支持高危端口、安全漏洞、高危应用等资产风险的发现； 3、支持验证风险可被利用性，并提供修复建议。

附件 2

信息技术服务商安全交付能力服务认证

检验评估机构申请书模板（试行）

申请机构名称：_____

申 请 日 期：_____

填报须知

1. 检验评估机构在正式填写本《申请书》前，须认真阅读并理解以下内容。

2. 检验评估机构应如实、详细地填写本《申请书》所有内容。

3. 检验评估机构应按照本《申请书》原有格式进行填写，不得更改格式和内容。如填写内容较多，页数不够时可用 A4 纸附页。

4. 检验评估机构须提交本《申请书》(含附件及证明材料)纸版一份（A4 纸双面打印，字迹清楚），要求盖章的地方，必须加盖公章。

5. 本《申请书》所选“□”内打“√”。

6. 本《申请书》要求提供的附件及证明材料须单独装订成册并编目。提供的资料须客观、真实和完整，不要编辑、修改和摘录，但可以进行脱敏处理。

检验评估机构声明

本单位正式提出检验评估机构申请,愿意按照认证中心的有关程序和管理规则要求,接受全过程监督管理。如本单位合作资格被暂停或撤销,承诺立即停止使用全部相关标识及宣传材料。同时作出以下承诺:

1、本单位所提供的申请书中一切信息以及整个过程中提供的信息真实、准确;

2、本单位承诺将自觉遵守认证相关法律法规要求,确保本检验评估机构相关工作合法合规;

3、本单位自愿向认证中心提供信息技术服务商安全交付能力服务认证工作所需必要信息和资料,按照认证中心的有关程序和管理规则要求,自愿接受认证中心的监督。

申请检验评估机构法定代表人/被授权人签名:

申请检验评估机构(盖章):

年 月 日

一、 检验评估机构基本信息

<table>
<tr><td>名称</td><td colspan="4"></td></tr>
<tr><td>注册地址</td><td colspan="4"></td></tr>
<tr><td>场所</td><td colspan="4"></td></tr>
<tr><td>组织机构代码/统一社会信用代码</td><td colspan="4"></td></tr>
<tr><td>法律地位</td><td colspan="4">☐独立法人 ☐非独立法人</td></tr>
<tr><td colspan="5">检验评估机构所在具有法人资格的机构名称（若是独立法人单位此项不填，否则填写附件1）：</td></tr>
<tr><td rowspan="2">检验评估机构负责人</td><td>姓名</td><td></td><td>职务</td><td></td></tr>
<tr><td>电话</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="2">授权签字人（报告批准人）</td><td>姓 名</td><td></td><td>职 务</td><td></td></tr>
<tr><td>电 话</td><td></td><td>传 真</td><td></td></tr>
<tr><td>检验评估机构所属行业类别</td><td colspan="4">☐公共通信和信息服务 ☐能源 ☐交通 ☐水利 ☐金融 ☐公共服务 ☐电子政务 ☐国防科技工业 ☐公共安全 ☐其他</td></tr>
<tr><td>资质情况</td><td colspan="4">☐中国合格评定国家认可委员会检验机构认可证书
☐中国合格评定国家认可委员会实验室认可证书
☐检验检测机构资质认定证书
☐其他</td></tr>
</table>

注：1.检验评估机构的申请主体须与中国合格评定国家认可委员会检验机构/实验室认可证书主体一致；

2.授权签字人（报告批准人）填写可根据检验评估机构自身情况进行增行。

二、提交文件清单

1、申请机构或母体的营业执照副本复印件及非独立法人授权书（参照附件1）；

2、法定代表人、主要负责人等为中华人民共和国境内的中国公民及无犯罪记录的证明；

3、信用记录查询结果截图，所有截图应包含查询网址、查询日期及完整的查询结果页面；

a. “信用中国”网站（www.creditchina.gov.cn）：企业完整信用信息详情截图；失信被执行人查询结果截图；重大税收违法失信主体查询结果截图；

b. 中国政府采购网（www.ccgp.gov.cn）：政府采购严重违法失信行为记录名单查询结果截图；

4、中国合格评定国家认可委员会检验机构/实验室认可证书及认可的能力范围（并标注管理规则 4.1 e 条要求相关的能力范围）；

5、关键信息基础设施保护工作部门或关键信息基础设施运营者出具的书面推荐材料（至少包括：对被推荐方的专业评价；由推荐单位主要负责人亲笔签字并加盖推荐单位公章；推荐信自签发之日起6个月内有效。）

6、公正性与独立性声明（加盖公章）：依据管理规则 4.2 公正性与独立性要求，给出声明并加盖公章；

7、保密制度及发布、实施、评审记录；

8、提供检验评估人员情况表（见附件2），检验评估机构人员简历（近

6个月社保记录、劳动合同、专业背景、专业资质、工作经验等）；

9、检验评估机构租赁合同或房产证等复印件、检验评估机构平面图及现场图片（包含消防安全情况、物理访问措施、功能分区）等；

10、提供检验评估设备及工具列表（见附件3）及对应的设备和工具检测报告、定期漏洞更新与安全验证记录、租用借用合同及设备和工具管理制度等；

11、检验评估机构现行有效的质量手册（如有）和程序文件（或其他称谓）及实施、发布、评审记录等；

12、以往的项目案例及脱敏的报告。

附件 1：

非独立法人授权书（加盖公章，模板可修改）

为确保被授权方独立、客观、公正地开展信息技术服务商安全交付能力服务认证检验评估业务，授权方在此作出如下授权与承诺：

一、独立授权声明

母体机构（授权方）特此全权授权该非独立法人检验评估机构（被授权方）独立开展以下检验评估业务：

被授权方在授权范围内，可独立出具评估报告等相关技术文件。

二、业务关系界定与隔离承诺

授权方承诺严格区分被授权方所从事的评估活动与母体机构其他业务活动，确保两类业务在组织架构、业务流程、人员安排、资金管理等方面相互隔离,防止利益冲突和母体机构其他业务对评估活动造成不当干预。

三、独立性及公正性保障承诺

授权方郑重承诺，始终保障被授权方在人员选派、财务管理、技术决策、结果判断等方面的独立性，绝不实施任何可能影响其评估公正性的行为，包括但不限于行政指令、经济诱导、关系干扰等，确保其评估活动客观、公正。

四、资源保障承诺

授权方承诺持续为被授权方提供独立有效开展评估业务所必需的人力、财务、设备、技术及信息等资源支持，确保其具备相应资质能力和工作条件。

五、最终法律责任承担

授权方明确承认并承诺,对被授权方在本次授权范围内开展评估业务

所产生的一切法律责任（包括但不限于民事、行政、刑事责任），最终由授权方承担。

本授权书自签署之日起生效，长期有效，直至授权关系依法变更或终止。

授权方：

法定代表人（或授权代表）签字：

日期：_____年_____月_____日

被授权方：

负责人签字：

日期：_____年_____月_____日

附件 2：

检验评估人员情况表

序号	姓名	年龄	职称	学历	所学专业	岗位	从事检验评估工作年限	检验评估人员类型
								授权签字人/专业分析人员/技术测试人员

注：1、根据情况自行增添表格行数，检验评估人员情况表应与随本申请书提交的人员简历一致；

2、人员应当满足 4.3 相关要求，评估人员总数不少于 15 人。

附件 3：

检验评估设备及工具列表

序号	名称	型号/版本	工具资质	生产企业	主要功能	工具产权方	备注

注：1、工具形态可在备注中注明，如软件、硬件等。