国家信息安全测评

信息安全服务资质申请与维持指南

（人工智能安全类一级）

CNITSEC

2026 年 6 月

目　录

引　言

中国信息安全测评中心（以下简称测评中心）是中央批准成立的国家信息安全权威测评机构，以“为信息技术安全性提供测评服务”为宗旨。

依据中央授权，测评中心的主要职能是：

1. 开展信息安全漏洞分析与风险评估；
2. 开展信息技术产品、系统和工程建设的安全性测试与评估；
3. 开展信息安全服务和信息安全专业人员的能力评估与资质测评；
4. 开展信息安全技术咨询、工程监理与开发服务；
5. 从事信息安全测试评估的理论研究、技术研发、标准研制；
6. 出版《中国信息安全》杂志等。

“信息安全服务资质认定”是对信息安全服务提供者的技术、资源、法律、管理等方面的资质、能力和稳定性、可靠性进行评估，依据公开的标准和程序，对其安全服务保障能力进行评定和确认。为我国信息安全服务行业的发展和政府主管部门的信息安全管理以及全社会选择信息安全服务提供一种独立、公正的评判依据。

欢迎关注国家信息安全服务资质官方微信号

一、 认定依据

信息安全服务（人工智能安全类）资质认定是对人工智能安全服务提供者的资格状况、技术实力和人工智能安全实施过程、质量保证能力等方面开展综合评价。在技术能力评定环节，参考人工智能应用领域现行国家标准、行业标准列明的各项技术指标与安全管控要求，作为技术能力审核、安全实施成效核验的重要评定依据。

信息安全服务（人工智能安全类）资质级别的认定，是依据《信息安全服务资质评估准则》和对应级别的信息安全服务（人工智能安全类）资质具体要求，在对申请单位的基本资格、技术实力、人工智能安全服务能力以及人工智能安全项目的组织管理水平等方面进行综合评定后，由测评中心给予相应的资质级别认定。

二、 级别划分

信息安全服务（人工智能安全类）资质认定是对人工智能安全服务提供者的综合实力的客观评价和确认，信息安全服务（人工智能安全类）资质级别体现了人工智能安全服务主体服务保障能力的成熟程度。

信息安全服务资质依照国家标准 GB/T 20261-2020《信息安全技术 系统安全工程能力成熟度模型》的能力等级，设为五个级别，一级到五级能力递增，五级为最高级别。

一级：基本执行级

二级：计划跟踪级

三级：充分定义级

四级：量化控制级

五级：持续改进级

三、 一级资质要求

申请单位需要在基本资格和基本能力、人工智能安全过程能力和项目与组织过程能力等几个方面符合《信息安全服务资质具体要求（人工智能安全类一级）》的规定。

3.1 基本资格要求

申请信息安全服务（人工智能安全类一级）资质的单位必须是一个独立的实体，原则上具有独立法人资格，遵守国家法律法规。

3.2 基本能力要求

3.2.1 组织与管理要求

1. 应依据组织管理制度，为持续的人工智能安全服务提供组织保障；
2. 应具有专业从事人工智能安全服务的队伍和相应的质量保证措施；
3. 应与人工智能安全服务相关的所有成员要签订保密合同，并遵守法律法规，履行保密责任。

3.2.2 技术能力要求

1. 了解人工智能安全技术的最新动向，具有掌握人工智能安全技术的能力；
2. 具有不断技术更新的能力；
3. 具有对人工智能安全面临的安全威胁、存在的安全隐患进行信息收集、识别、分析和提供防范措施的能力；
4. 具有对发生的安全事件进行分析和解决的能力；
5. 具有根据服务业务的需求开发人工智能、产品或支持性工具的能力；
6. 具有对集成的人工智能安全进行检测和验证的能力；
7. 具有对大模型进行安全维护的能力；

8. 有跟踪、了解、掌握、应用国际、国家和行业标准的能力。

3.2.3 人员构成与素质要求

1. 具有充足的人力资源和合理的人员结构；
2. 所有与人工智能安全服务有关的管理和销售人员应具有一定的信息安全知识；
3. 有相对稳定的从事人工智能安全服务的技术队伍；
4. 技术骨干人员应系统地掌握人工智能安全基础理论，并有一定的工作经验；
5. 拥有专职的注册信息安全专业人员不少于 4 名。

3.2.4 设备、设施与环境要求

1. 具有固定的工作场所和良好的工作环境；
2. 具有先进的开发、测试或模拟环境；
3. 具有先进的开发、生产和测试设备；
4. 具有实施相关服务必需的开发、生产和测试工具；
5. 模型及应用开发和运行环境安全有较好保障。

3.2.5 规模与资产要求

1.有足够的注册资金和充足的流动资金；
2.具有与所申请安全服务业务范围、承担的人工智能安全规模相适应的服务体系；
3.有足够的人员从事直接与人工智能安全服务相关的活动。

3.2.6 业绩要求

1.应具有从事人工智能安全服务的经验；
2.近 2 年内在人工智能安全服务方面，没有出现项目验收未通过的情况。

3.3 人工智能安全过程能力要求

人工智能安全过程能力，是衡量申请单位人工智能安全服务专业水平的核心指标。

申请单位应能实施以下 12 个人工智能安全过程域：

（一）保障基座和模型安全的能力

1. 基座和模型全生命周期安全管控能力；
2. 评估基座训练环境与基础设施安全的能力；
3. 评估模型安全风险检测与应急处置的能力；

（二）保障数据安全的能力

4. 数据全流程安全管控的能力；
5. 开展数据分级分类与权限管控的能力；
6. 开展数据安全合规核查能的能力；

（三）保障运行环境安全的能力

7. 具备运行环境安全隔离与防护的能力；
8. 具备运行环境安全监测与漏洞修复的能力；
9. 具备运行环境应急响应与恢复的能力；

（四）保障应用安全的能力

10. 具备应用全流程安全管控的能力；
11. 保障内容安全与生成内容管控的能力；
12. 具备应用安全风险监测与拦截的能力。

3.4 项目和组织过程能力要求

项目和组织过程能力，是衡量人工智能安全服务规范性和质量保证成熟度的重要。

申请单位应能实施以下 6 个项目和组织过程域：

1. 实现质量保证的能力；
2. 管理项目风险的能力；
3. 规划技术活动的能力；

4. 监控技术活动的能力；

5. 提供不断发展的知识和技能的能力；

6. 与供应商协调的能力。

四、 申请准备

申请单位需要到测评中心网站（https://www.itsec.gov.cn）查看并下载《信息安全服务资质评估准则》《信息安全服务资质申请与维持指南（人工智能安全类一级）》和《信息安全服务资质申请书（人工智能安全类一级）》及相关附件，认真阅读上述文档，了解资质认定的流程及相关情况，确定本单位满足一级资质的基本资格和基本能力要求。

申请单位根据相关要求填写申请书（人工智能安全类一级）、加盖公章并装订后，将申请书及所要求的相关资料刻光盘或 U 盘，一并以快递方式邮寄至测评中心。正式递交前，申请单位须逐项检查所填报的材料的完整性和正确性。

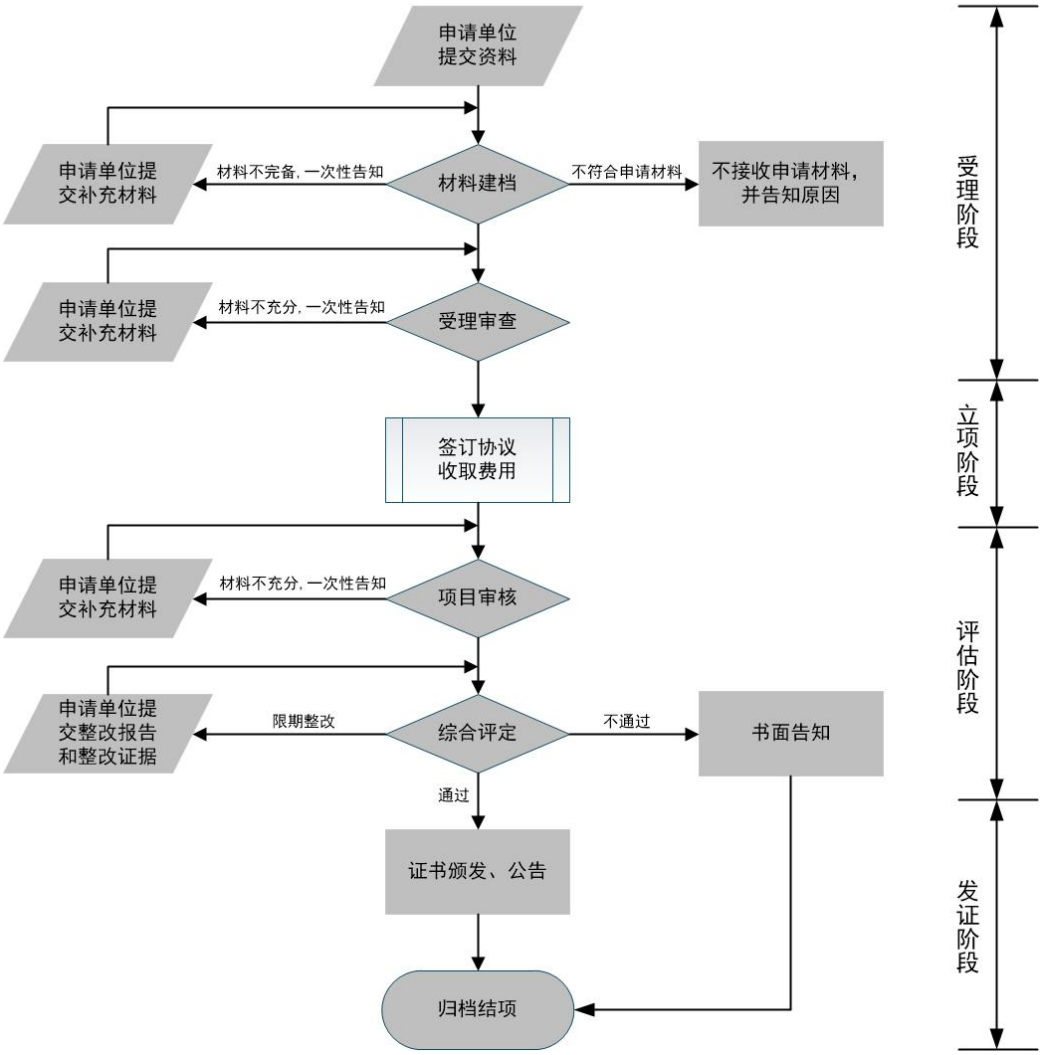
如申请单位已获得该类别服务资质证书，至少需要在证书有效期届满前六个月，提交该类型资质相关材料维持原有级别申请。证书有效期届满超六个月后提交维持申请的，视作初次申请。维持申请流程与首次申请流程一致。

申请单位可在测评中心网站或“国家信息安全服务资质”公众号上阅读《信息安全服务资质申请常见问题解答》了解更多信息。

联系方式详见第十章。

五、 资质认定

5.1 项目实施流程图



5.2 受理阶段

申请单位资料建档立项应满足以下三个条件：（一）申请单位必须是一个独立的实体，原则上具有独立法人资格；（二）申请书加盖申请单位公章且装订成册；（三）随附电子版资料。

项目负责人对申请资料的形式规范度、申请单位的基本资格、基本能力、专项技术过程能力和组织管理能力进行受理审查，判定证据的充分性，一般以电子邮件形式反馈受理审查意见。

5.3 立项阶段

项目负责人按照测评中心合同管理要求起草制式委托协议，依据收费标准确定委托测评费用，以电子邮箱发送协议及相关附件模板至申请单位指定电子邮箱，邮件中说明协议和附件的填写要求。

委托协议生效，且申请单位支付委托测评费用后，项目进入评估阶段。

5.4 评估阶段

项目组与申请单位充分沟通，拟定审核计划，进行评估准备。

项目组按照审核计划，开展评估活动。评估方式包括但不限于文档审查、人员访谈、实际操作等。

a) 文档审查。通过审查申请单位相关文档，例如：实施记录、报告、数据等，掌握人工智能安全服务活动的开展情况；

b) 人员访谈。通过访谈的方式与申请单位进行交流和讨论，获取人工智能安全服务相关信息，掌握具体执行过程；

c) 实际操作。通过演示和操作人工智能安全服务活动所必须的工具、平台及测试环境等，掌握申请单位的实施能力。

项目组根据采集的证据，对申请单位的人工智能安全服务能力符合程度进行评估，给出项目审核结论。

专家组对该项目证据的充分性，审核结论的合理性，进行综合评定，形成专

家评审结论。评审结论为通过的项目进入发证阶段。

5.5 发证阶段

制证工作人员依照测评中心证书发放及公告的审批流程，按批次制作证书并及时发放，申请单位获证信息在测评中心网站、《中国信息安全》杂志、“国家信息安全服务资质”公众号上予以公告。

六、 处置

申请单位存在违规行为时，测评中心有权视申请单位违规情节轻重予以以下处置：警告、限期整改、暂停证书、取消证书。

七、 争议、投诉与申诉

申请单位对测评中心所作评审结论有异议时，可向测评中心提出书面申诉。测评中心监督部门负责进行调查，并给出调查结论。

申请单位应妥善处理因自身行为而发生的投诉，保留记录并采取措施防止问题的再发生。测评中心监督部门将在必要时查阅申请单位的投诉或申诉记录。

八、 申请单位档案

申请单位的项目档案归档保存六年。

九、 费用及周期

1. 首次获得一级资质证书费用：

   21000（审核费用）+15000（三年年金）＝36000 元

2. 维持一级资质证书费用：

   21000（审核费用）+15000（三年年金）＝36000 元

3. 项目实施周期原则上不超过六个月。周期时间不包含申请单位补充资料、协议审批生效及支付费用等时间。

十、 联系方式

名　称：中国信息安全测评中心 资质评估处

地　址：中国北京市海淀区上地西路 8 号院 1 号楼（邮编：100085）

咨询电话：010-82341582 或 82341551

测评中心网站：https://www.itsec.gov.cn

服务资质公众号：国家信息安全服务资质

欢迎关注国家信息安全服务资质官方微信号