



生成式人工智能服务安全认证实施规则

CQC/SSGZ GAIS0001-2025

生成式人工智能服务安全认证实施规则 (版本号: A/2)



2025年9月17日发布 2026年5月27日修订 2026年5月27日实施

中国质量认证中心



前 言

本规则由中国质量认证中心发布，规则相关的知识产权归中国质量认证中心所有，任何组织及个人未经中国质量认证中心许可，不得以任何形式全部或部分使用。





目 录

前 言	I
1 目的和适用范围	1
2 认证依据	1
3 认证范围	1
4 认证类别/领域划分	1
5 认证单元划分	1
6 样本选取方案	2
7 认证模式	2
8 认证实施程序	3
8.1 认证申请受理	3
8.2 申请评审	3
8.3 再认证、证书变更的评审	4
8.4 周期的确定	4
8.5 认证方案策划	4
8.6 初次认证的审查程序	4
8.7 审查结论	5
8.8 审查报告的编制、批准和分发	6
8.9 材料归档/上报	6
8.10 认证复核、决定及证明	6
8.11 获证后保持认证	6
8.12 再认证程序	6
8.13 应急准备与响应措施	6
9 认证变更	7
10 认证评价和结果	7
10.1 认证评价	7
10.2 认证结果	7
11 认证证书状态管理规定	7
11.1 暂停	7
11.2 恢复	7
11.3 撤销	7
11.4 注销	7
12 认证证书及标志要求	8
12.1 认证证书	8
12.2 认证标志	9
13 审查人日数	9

1 目的和适用范围

为规范生成式人工智能服务安全认证工作，确保认证活动的公正性、规范性和有效性，依据《中华人民共和国认证认可条例》、《认证机构管理办法》、GB/T 27065 《合格评定 产品、过程和服务认证机构要求》、《生成式人工智能服务管理暂行办法》、GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》等法规和规范性文件，制定本规则。

本规则对生成式人工智能服务安全认证的适用范围、认证依据、认证范围、实施程序、证书及标志要求、证书状态管理等作出规定，并明确认证模式、认证领域、单元划分、样本选取（抽样）等，适用于所有自愿申请生成式人工智能服务安全认证的组织（以下简称“申请组织”）。

本规则适用于生成式人工智能服务安全认证。

2 认证依据

GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》

3 认证范围

本规则适用于生成式人工智能提供的服务，认证范围依据组织服务活动涉及服务生成内容的模态、大模型名称及版本、涉及的服务场景进行详细界定。

4 认证类别/领域划分

认证类别：服务认证；

认证领域：SC12 电信服务；信息检索和提供服务。

5 认证单元划分

同一生成式人工智能服务组织、提供生成同一模态内容的服务，界定为同一认证单元。根据生成式人工智能服务模态的特点，其认证单元划分如下：

序号	认证单元名称	认证单元说明	认证依据
1	文本生成式人工智能服务	文本对话类生成式人工智能服务，如智能聊天助手，客服机器人，客服机器人等	GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》
2	图片生成式人工智能服务	图像与视觉内容生成类人工智能服务，如文生图、图像编辑与增强、风格迁移等	GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》
3	音频生成式人工智能服务	声音与音乐生成类人工智能服务，如语音合成、音乐创作、音效生成等	GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》
4	视频生成式人工智能服务	动态影像生成与编辑类人工智能服务，如文生视频、视频内容生成、视频编辑与特效等	GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》

5	其他生成式人工智能服务	其他不属于上述类别的生成式人工智能服务，如三维模型生成等	GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》
---	-------------	------------------------------	---

6 样本选取方案

6.1 样本选取

根据申请组织生成式人工智能服务安全认证单元的特点和认证模式的选择, 考虑样本的选择, 并关注训练数据和模型输出内容:

(1) 训练数据抽样

- a) 人工抽检从全部训练数据中随机抽取不少于4000条训练数据。
- b) 关键词抽检、分类模型抽检总计从全部训练数据中随机抽取不少于总量10%的训练数据。

(2) 模型输出内容测试题抽样

- a) 生成内容测试题库中随机抽取不少于1000道题生成内容测试题库中随机抽取不少于1000道题。
- b) 测试从拒答测试题库中随机抽取不少于300道题

7 认证模式

7.1 认证模式组合

本服务认证遵循“初次认证 + 保持认证（监督）”的组合方式，适用的服务认证模式(由一种或多种认证模式组成) 包括：

代码	可选的认证模式
A	公开服务特性检验
C	公开服务特性检测
G	服务能力确认/验证
H	服务设计审核
I	服务管理审核

a) 初次认证

初次认证由文件评审+技术测评+现场审查组成，采用A+C（技术测评）+G+H（如有）+I模式。

b) 保持认证（监督审查）

保持认证期间，每年实施一次现场监督审查，每次监督审查至少覆盖A+C（技术测评）+H（如有）+G+I模式，并重点关注初次认证或再认证中识别的风险点

c) 再认证

再认证应在证书到期前进行，认证模式与初次认证一致。

本文件由中国质量认证中心有限公司制定、发布。未经许可，不得以任何形式全部或部分转载、使用本文件。

如需查看全文，请联系中国质量认证中心 罗恒中，联系电话：
010-83886812，联系邮箱：luohengzhong@cqc.com.cn。