

# 注册人工智能安全评估专业人员 (CISP-AISA)

## 白皮书

发布日期 2026 年 6 月



**CNITSEC**

版本：V1.0

中国信息安全测评中心

奇安信网神信息技术（北京）股份有限公司

©版权 2026-中国信息安全测评中心

目 录

引言 ..... 1

一、 CISP-AISA 介绍 ..... 2

二、 CISP-AISA 考试培训内容 ..... 3

三、 CISP-AISA 注册与维持 ..... 5

四、 CISP-AISA 注册流程 ..... 6

五、 CISP-AISA 收费标准 ..... 8

六、 CISP-AISA 维持要求 ..... 9

七、 CISP 职业准则 ..... 10

## 引言

当前，以大模型为核心的人工智能技术发展势头强劲、持续快速迭代，正在给全球经济、科技与社会领域带来巨大的变化，既是拉动产业发展的重要动力，也不断重塑产业形态与大众生产生活模式，而且发展格局逐步明晰，国家间竞争范围从基础模型研发、场景应用，拓展到算力、数据、高端芯片、专业人才等关键领域。人工智能热潮还重塑了全球经贸与资本流向，已然成为影响国际地缘政治局势的重要力量。

人工智能高速发展的背后，各类安全隐患随之凸显，安全问题已然成为行业稳步发展的突出阻碍。当前人工智能领域极易遭遇网络攻击、数据泄露、信息滥用等诸多风险，不仅会造成经济损失，还会危及公共秩序与国家信息安全，拖累行业创新发展。想要守住人工智能安全底线，有效平衡技术发展与风险管控，充分发挥智能技术价值，就必须重视人工智能安全建设，大力培育兼具专业素养与实操能力的行业技术人才，补齐安全领域人才缺口。

为了更好的培养和选拔人工智能安全评估相关岗位的优秀人才，中国信息安全测评中心推出了“注册人工智能安全评估专业人员”（CISP-AISA）技术能力水平认证考试，引导广大网络信息安全工作者学习和研究人工智能方向的安全评估相关知识、课题、技术方法，从而帮助国内各政企、事业单位的人工智能安全防御能力有效提升，为我国人工智能安全的发展作出积极的贡献。

## 一、 CISP-AISA 介绍

注册人工智能安全评估专业人员，英文名称 Certified Information Security Professional – Artificial Intelligence Security Assessment，简称 CISP-AISA，是面向网络信息安全企业、网络信息安全咨询服务机构、网络信息安全测评机构、政府机构、社会各组织、团体、大专院校以及企事业单位中负责人工智能系统安全检测、安全评估、安全防御等人工智能安全技术专业人员所颁发的专业资质证书。证书持有人主要从事以大语言模型为主要对象的人工智能安全评估工作，具有识别人工智能大模型面临的安全威胁与风险、能够对人工智能大模型自身及其应用、组件、内容进行安全评估的能力。

CISP-AISA 专业资质适用于以下人员：

- ✓ AI 安全测评人员：等保测评师、网络安全厂商的 AI 安全测试工程师；
- ✓ AI 安全合规审计人员：工作对象涉及到 AI 的安全合规审计人员、安全治理人员；
- ✓ AI 安全监管人员：从事 AI 安全监管、安全核查的工作人员；
- ✓ AI 安全咨询人员：工作对象涉及到 AI 的安全咨询顾问；
- ✓ AI 应用开发人员：政企、特别是关基单位的 AI 应用产品经理、AI 应用研发人员、AI 应用运营管理人员。

## 二、 CISP-AISA 考试培训内容

CISP-AISA 认证考试旨在培养和锻炼考生具备独立进行人工智能大模型安全评估的能力，有效增强我国人工智能安全评估领域的人才储备，促进国家企事业单位人工智能安全防御能力不断提高，在人工智能安全评估领域能够发现人才、选拔优秀人才而设立的技能水平考试。

考试内容从多个知识类角度出发，通过客观题目与上机实际操作题目相结合的形式，来考核考生的能力。考生需要了解当前人工智能发展阶段面临的主要安全问题，跟踪人工智能安全发展动态，能够在当前真实的人工智能应用环境中通过技术评估手段发现和解决人工智能大模型安全问题。

CISP-AISA 培训课程讲解的内容包括：AI 基础概念、核心要素、关键技术及安全特性，了解 AI 的国内外应用发展现状，AI 安全风险框架；国内 AI 安全国家战略及落地路径，国内外相关法规政策、执法情况，国际与国内人工智能安全标准规范；人工智能大模型的数据、模型自身、应用及基础设施等技术安全威胁，大模型生成内容合规风险，认知对抗与社会工程类内容安全风险；大模型交互、检索增强生成、智能体等应用、大模型应用、组件、自身及内容的安全评估技术与方法；大模型服务与交互层防御、网关安全围栏、模型本体加固、应用逻辑与运营层防御、智能体业务风控及 LLM0ps 安全运营与应急处置等方面的技术知识；AI 安全评估报告编写方法。

通过以上内容的学习，要求考生可以结合教学中及实际工作中的典型案例，掌握更多的人工智能安全评估工作所需方法与技能，提高个人的相关技术能力。具备人工智能安全评估相关岗位人员应有的技术能力与职业素养。

以下为 CISP-AISA 的知识体系结构框架：



**CISP-AISA知识体系结构框架**

具体考试内容、知识范围及考试知识域分布，请从官方下载《注册人工智能安全评估专业人员（CISP-AISA）知识体系大纲》进行阅读了解。

### 三、 CISP-AISA 注册与维持

成为注册人工智能安全评估专业人员（CISP-AISA），必须同时满足以下基本要求：

1、申请成为注册人工智能安全评估专业人员（CISP-AISA），要求具备一定人工智能大模型相关基础知识及网络安全相关基础知识，有意向从事人工智能安全评估相关工作的人员。

2、申请成为注册人工智能安全评估专业人员（CISP-AISA），无学历与工作经验的报考要求；

3、申请参加考试前，须参加 CISP-AISA 授权培训机构的培训，完成相关的学习，掌握考试大纲中要求的人工智能安全评估相关知识与实际操作能力。

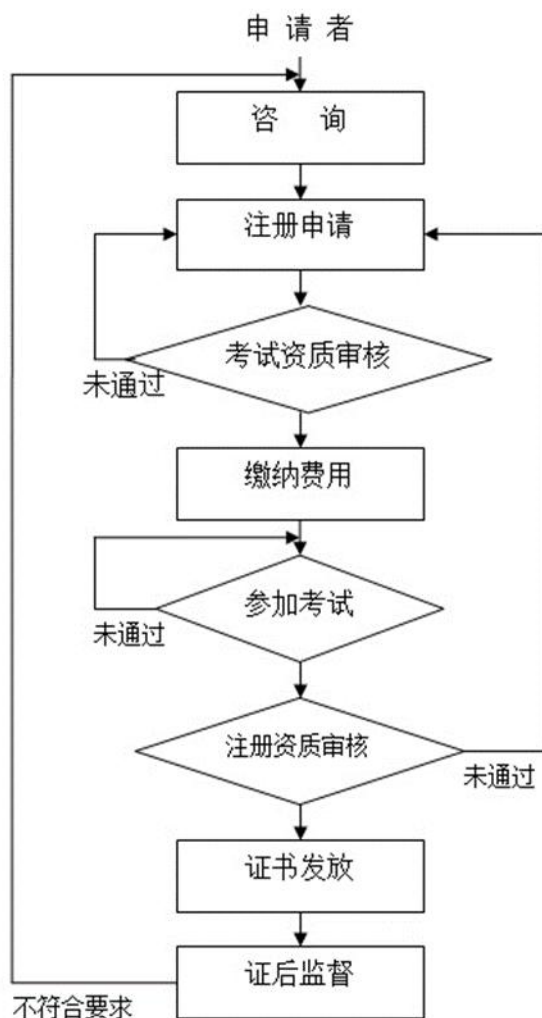
4、通过 CISP-AISA 运营中心组织的 CISP-AISA 认证考试；

5、同意并遵守 CISP 职业道德准则；

注册人工智能安全评估专业人员（CISP-AISA）资质证书的有效期为三年，证书失效后，维持证书时需参加 CISP-AISA 维持考试。

## 四、 CISP-AISA 注册流程

CISP-AISA 的注册流程如下图所示，共分为 3 个步骤：



**CISP-AISA注册流程**

### 第一阶段：咨询、申请与初审

1. 咨询与申请：申请者向授权培训机构咨询，并提交注册申请；
2. 资质初审：授权运营中心对申请者进行考试资质审核，审核未通过重新提交注册申请；审核通过后，进入下一个阶段；

### 第二阶段：缴费、培训与考试

1. 缴纳费用：申请者根据要求缴纳相关费用；
2. 参加培训：完成缴费后，参加授权培训机构组织的培训；



3. 参加考试：培训完成后，按照统一安排参加中国信息安全测评中心组织的考试，考试结果未通过需要进行补考；通过进入下一个阶段；

### **第三阶段：获证、证后监督**

获得证书：管理部门对考试通过者进行最终注册资质审核，未通过审核者需重新提交注册申请；审核通过者将获得中国信息安全测评中心颁发的资质证书并接受证后监督。

## 五、 CISP-AISA 收费标准

### 1. CISP-AISA 收费标准

| 收费种类     | 收费金额（元/人）    |
|----------|--------------|
| 建议培训费    | 9800         |
| 培训管理及考试费 | 4000         |
| 注册费      | 500          |
| 注册年金（三年） | 1500         |
| 合计       | <b>15800</b> |
| 补考费      | 3000         |

每位考生初次缴纳考试费后，拥有参加初次考试及两次免费补考共三次考试机会。如初次考试及两次补考均未通过，则后续再参加补考时需缴纳补考费。

## 六、 CISP-AISA 维持要求

### 6.1、CISP-AISA 维持考试介绍

持有 CISP-AISA 资质的人员，当证书有效期届满三年、需要进行资质维持时，须参加 CISP-AISA 注册资质维持测评考试，且考试成绩合格，经中国信息安全测评中心审核通过后，方可办理资质维持续证。

CISP-AISA 证书超期 6 年以上不予维持，需要重新参加 CISP-AISA 注册考试。

如果参加维持考试成绩未通过，可以申请补考，直至考试通过。每位考生有两次免费补考机会，前两次补考不需要缴纳补考费，如两次补考均未通过，则从第三次补考开始，需要缴纳补考费后方可进行补考。

### 6.2、CISP-AISA 维持考试费用

#### ● 维持考试费

| 维持考试类别    | 维持考试费  |
|-----------|--------|
| CISP-AISA | 3750 元 |

#### ● 维持考试补考费

| 维持考试补考类别  | 维持考试补考费 |
|-----------|---------|
| CISP-AISA | 1875 元  |

#### ● 超期维持费

CISP 及包括 CISP-AISA 在内的子品牌资质证书，超过有效期 6 个月以上，收取证书维持超期费用，超期维持费用为 500 元/年（超期 6 个月不足 12 个月的按照一年收取）。

## 七、 CISP 职业准则

作为国家注册信息安全专业人员应该遵循其应有的道德准则，中国信息安全测评中心为CISP注册人员设定了职业道德准则。

### 1. 维护国家、社会和公众的信息安全；

自觉维护国家信息安全，拒绝并抵制泄露国家秘密和破坏国家信息基础设施的行为；

自觉维护网络社会安全，拒绝并抵制通过计算机网络系统谋取非法利益和破坏社会和谐的行为；

自觉维护公众信息安全，拒绝并抵制通过计算机网络系统侵犯公众合法权益和泄露个人隐私的行为。

### 2. 诚实守信，遵纪守法

自觉遵守国家相关法律、法规；

不通过计算机网络系统进行造谣、欺诈、诽谤、弄虚作假等违反诚信原则的行为；

不利用个人的信息安全技术能力实施或组织各种违法犯罪行为；

不在公众网络传播反动、暴力、黄色、低俗信息及非法软件。

### 3. 努力工作，尽职尽责

热爱信息安全工作岗位，充分认识信息安全专业工作的责任和使命；

为发现和消除本单位或雇主的信息系统安全风险做出应有的努力和贡献；

帮助和指导信息安全同行提升信息安全保障知识和能力，为有需要的人谨慎负责地提出应对信息安全问题的建议和帮助。

### 4. 发展自身，维护荣誉

通过持续学习保持并提升自身的信息安全知识；

利用日常工作、学术交流等各种方式保持和提升信息安全实践能力；

以CISP身份为荣，积极参与各种证后活动，避免任何损害CISP声誉形象的行为。