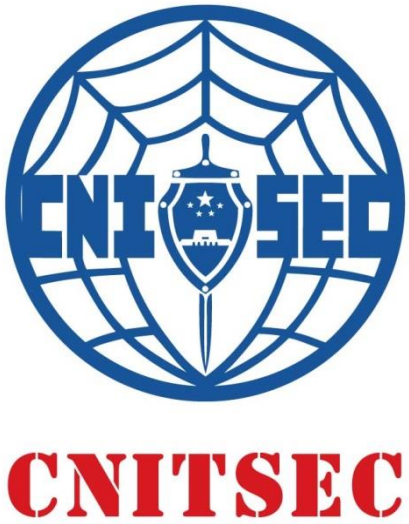
# 注册信息安全专业人员

# 应急响应方向（IRE、IRS）

# 白皮书

发布日期：2022 年 11 月




**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**

# CISP-IRE/CISP-IRS 白皮书

## 咨询及索取

关于中国信息安全测评中心 CISP-IRE/CISP-IRS 考试相关的更多信息，请与注册信息安全专业人员攻防领域考试中心联系。

注册信息安全专业人员攻防领域考试中心联系方式

【邮　　箱】CISP@qianxin.com

【地　　址】北京市西城区西直门外大街 136 号新动力金融科技中心 7 层

【邮　　编】100044

奇安信集团下属的奇安信网神信息技术（北京）股份有限公司是以“保护大数据时代的安全”为企业使命，以“数据驱动安全”为技术思想，专注于为政府和企业提供新一代网络安全产品和信息安全服务的提供商。奇安信集团与中国信息安全测评中心联合成立注册信息安全专业人员攻防领域考试中心，由奇安信集团子公司奇安信网神信息技术（北京）股份有限公司具体运营，负责注册信息安全专业人员应急响应工程师（CISP-IRE）资质及注册信息安全专业人员应急响应专家（CISP-IRS）资质的培训知识体系制定、考试系统开发维护、业务推广指导、市场宣传支持及持证人员的服务。CISP 攻防领域注册考试，专注于培养、考核高级实用型网络安全渗透测试方向与应急响应方向专业人才，是业界首个理论与实践相结合的网络安全专项技能水平实际操作能力考察注册考试。

# 目　录

# 引言

当前，信息化社会发展方兴未艾，信息成为一种重要的战略资源。信息的获取、存储、处理及其安全保障能力成为一个国家综合国力的重要组成部分。目前，信息产业已成为世界第一大产业，信息科学与技术正处于空前繁荣的阶段。信息安全是信息的影子，哪里有信息，哪里就有信息安全问题。在信息科学与技术发展欣欣向荣的同时，危害信息安全的事件也不断发生。

基于严峻的网络空间安全形势，国内外多位信息安全领域资深专家、学者指出：不断增长的产业链式网络攻击虽然日趋严重，但是更让人担忧的是，网络安全人才的短缺致使各个层级的网络安全团队难以“扩军”，信息安全领域人才的储备量远远跟不上网络安全风险的增长量。

网络安全人才决定网络安全技术的交替、更迭，而人才的短缺直接影响政府事业机关网络防御能力，也导致中、小型企业很难组建自己的安全团队。网络安全防范能力堪忧，严重影响我国网络安全建设。

《网络安全法》第三条提出 “国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。” 因此，培养“高素质的网络安全和信息化人才队伍”的工作刻不容缓！

- 中国信息安全测评中心主导的注册信息安全专业人员攻防领域考试中心推出的“CISP-IRE”（注册信息安全专业人员-应急响应工程师， Certified Information Security Professional - Incident Response Engineer）、“CISP-IRS”（注册信息安全专业人员-应急响应专家， Certified Information Security Professional - Incident Response specialist）技能水平注册考试，锻炼考生实际解决网络安全问题的能力，发现人才，有效增强网络安全防御能力，促进国家企事业单位网络防御能力不断提高。同时引导广大网络安全工作者在推动信息安全工作中建功立业，引导广大信息安全工作者在建设信息化强国过程中发挥中坚作用，引

导广大信息安全工作者在我国信息化建设与发展的征途中勇当先锋，团结动员广大网络安全从业者为我国网络安全建设又好又快地发展做出积极的贡献，为企、事业单位培养和选拔网络安全应急响应相关岗位的优秀人才。

# 一、CISP-IRE/CISP-IRS 考试要求

成为注册信息安全专业人员应急响应工程师（CISP-IRE）、注册信息安全专业人员应急响应专家（CISP-IRS），必须同时满足以下基本要求：

1、申请成为注册信息安全专业人员应急响应工程师（CISP-IRE），要求具备一定应急响应能力，或有意向从事应急响应的人员，包含信息安全相关专业高校生；申请成为注册信息安全专业人员应急响应专家（CISP-IRS），要求具备较强的应急响应和处理能力；

2、申请成为注册信息安全专业人员应急响应工程师（CISP-IRE）、注册信息安全专业人员应急响应专家（CISP-IRS）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 攻防领域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应急响应相关知识与实际操作能力；

4、通过注册信息安全专业人员攻防领域考试中心组织的 CISP-IRE、CISP-IRS 考试；

5、同意并遵守 CISP-IRE、CISP-IRS 职业道德准则；

6、满足以上 CISP-IRE、CISP-IRS 注册要求并成功通过 CISP-IRE、CISP-IRS 审核；

注册信息安全专业人员应急响应工程师/应急响应专家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-IRE、CISP-IRS 维持考试。

# 二、CISP-IRE/CISP-IRS 考试方向

该注册考试是为了锻炼考生实际解决网络安全问题的能力，有效增强我国网络安全防御能力，促进国家企事业单位网络防御能力不断提高，以发现人才，选

拔优秀人才而设立的技能水平考试。

考试内容从多个角度出发，通过客观题目与实际操作题目相结合（CISP-IRE）或全部为实际操作题（CISP-IRS）的形式，来考核考生的能力，通过多个得分点，对考生全面的考核，考生需要了解最新的网络安全技术，跟踪最新的网络安全动态，能够在真实的网络环境中发现问题和解决问题。同时，也可以为网络安全专业的学生提高自身价值和自身影响力，提供更好的学习素材，为更多热爱网络安技术、有志于从事网络安全事业的人员提供了一个更加具有优势的平台。

考生应理解网络安全事件和网络安全应急响应的正确概念，掌握安全事件的分类原则和分类方法。考生应该能够明确应急响应工作的目标，并且学会网络安全应急响应预案的制定方法，掌握应急响应的一般流程。

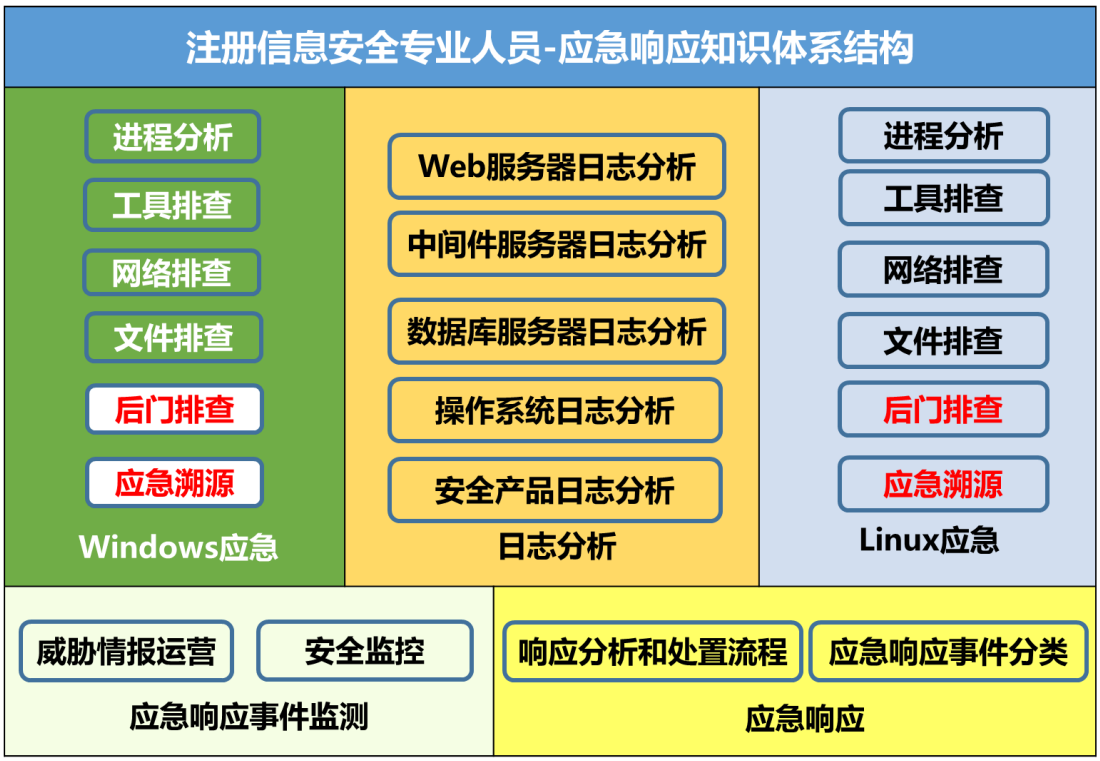
考生应了解和掌握网络安全应急响应的基础技术知识，包括 Windows 系统应急响应、Linux 系统应急响应、日志分析、应急响应常用工具使用等。能够正确、熟练的运用以上知识完成应急响应的基本工作。

考生应掌握应急响应事件监测的相关知识与能力，包括威胁情报运营与安全检测方法等。能够较好的完成应急响应检测相关工作。

考生应了解应急响应事件分析与处置的流程、掌握相关知识并运用到实际工作中。

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，掌握更多的网络安全应急响应工作所需安全技能，提高个人的相关技术能力。具备应急响应工程师应有的技术能力与职业素养。

下图为 CISP-IRE/ CISP-IRS 的知识体系结构框架：




**CISP-IRE/CISP-IRS知识体系结构框架**

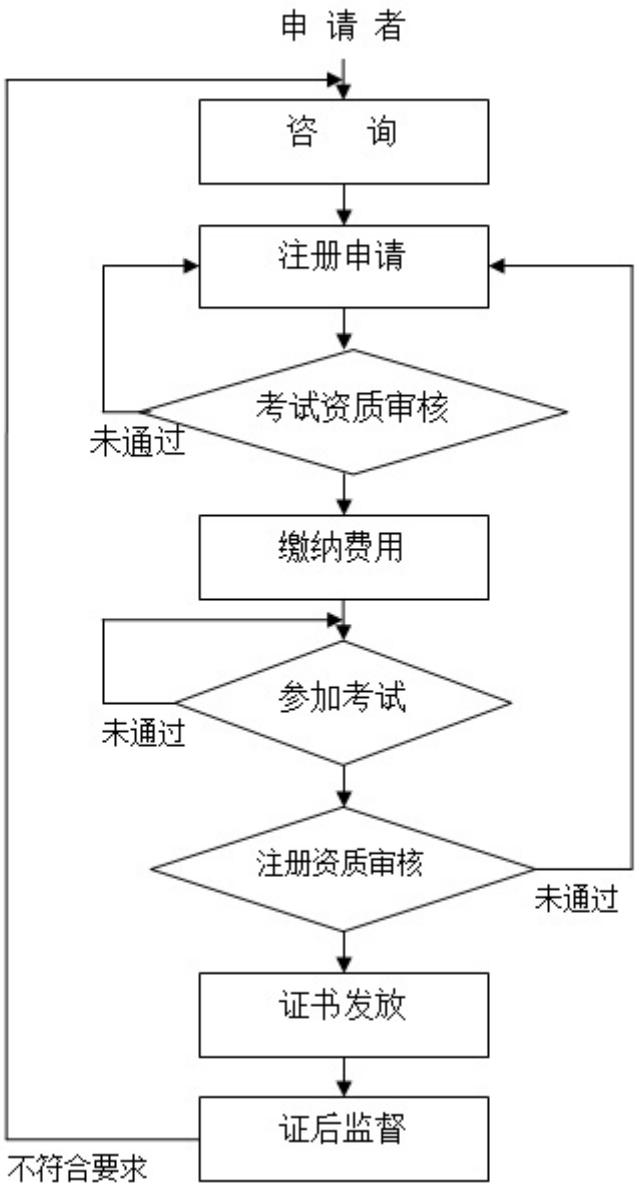
（注：其中红色字体为仅在 CISP-IRS 注册培训及考试中要求掌握的知识内容。）

为了确保授课质量，我们推荐的培训课程安排见下表，各授权培训机构也可根据需要自行调整。

| 序号 | CISP-IRE/CISP-IRS |
|---|---|
| 1 | 应急响应概况、流程、事件分类、计划制定 |
| 2 | 应急响应所需渗透测试知识、实操演练 |
| 3 | Windows 应急（IRE、IRS 分别要求掌握内容）、实操演练 |
| 4 | Linux 应急（IRE、IRS 分别要求掌握内容）、实操演练 |
| 5 | 日志分析、实操演练 |
| 6 | 应急响应事件监测、实操演练 |
| 7 | 应急响应事件分析与处置、实操演练 |

具体考试内容、范围及考试形式请下载《注册信息安全专业人员-应急响应方向（IRE、IRS）知识体系大纲》进行阅读了解。

# 三、CISP-IRE/CISP-IRS 注册流程



# 四、CISP-IRE/CISP-IRS 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

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。

# 五、CISP-IRE/CISP-IRS 考生申请资料要求

1.学员需要填写如下申请资料：

《注册信息安全专业人员（攻防领域）考试及注册申请表》

填写申请表格时应注意：申请表格可采用电子模版录入填写，也可手写，填写过程中应确保内容的真实准确，手写申请表格应用正楷字体，字迹要求清晰可辨。

**注：**填写注册申请表第二部分时，需要由申请人所在单位（部门）领导签字并加盖本单位公章。

2.申请（CISP-IRE/CISP-IRS）注册资质除了填写申请书外，还需要准备以下资料：

- 个人近期免冠 2 寸彩色**蓝底**证件照片 3 张（非蓝底照片为不合格照片，将不予采用）
- 身份证复印件 1 份

3.资料的提交时间

学员应在报名同时将所有资料全部提交。

# 六、CISP-IRE/CISP-IRS 收费标准

1．CISP-IRE 收费标准

单位：（元）

| 收费单位<br>收费种类 | 授权培训机构（元）/人 | 考试中心 | 合计 |
|---|---|---|---|
| 培训费 | 14800 | / | 14800 |
| 考试费 | / | 3000 | 3000 |
| 注册费 | / | 500 | 500 |
| 年金（三年） | / | 1500 | 1500 |
| 合计 | 14800 | 5000 | 19800 |
| 补考费 | / | 2500 | 2500 |

2、CISP-IRS 收费标准

单位：（元）

| 收费单位 / 收费种类 | 授权培训机构（元）/人 | 考试中心 | 合计 |
|---|---|---|---|
| 培训费 | 19800 | / | 19800 |
| 考试费 | / | 5500 | 5500 |
| 注册费 | / | 1000 | 1000 |
| 年金（三年） | / | 1500 | 1500 |
| 合计 | 19800 | 8000 | 27800 |
| 补考费 | / | 4000 | 4000 |

考试中心收费部分由报考人员选择委托的授权培训机构代缴纳，由奇安信网神信息技术（北京）股份有限公司先行代收，然后与中国信息安全测评中心统一结算。

3、收款单位账号

开户行：招商银行北京建国路支行

开户名：奇安信网神信息技术（北京）股份有限公司

账　号：110902261210404

# 七、注册信息安全专业人员攻防领域维持考试要求

## 1、CISP 攻防领域维持考试介绍

- **CISP 攻防领域维持考试服务对象**

CISP 攻防领域维持考试面向的服务对象为 CISP 攻防领域注册资质持有者，包括 CISP-PTE、CISP-PTS、CISP-IRE、CISP-IRS。

持有以上资质的人员，当证书有效期届满三年、需要进行资质维持时，须参加 CISP 攻防领域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 攻防领域维持考试申请**

CISP 攻防领域维持考试，由中国信息安全测评中心总体管理、监督与指导，由 CISP 攻防领域考试中心进行组织开展，由 CISP 攻防领域授权培训机构负责为维持人员提供咨询及提供报名申请服务。

只有经过 CISP 攻防领域考试中心授权、并经过中国信息安全测评中心审核批准的 CISP 攻防领域授权培训机构，才具有办理 CISP 攻防领域资质维持工作的资格。其它任何非授权培训机构，均无权代表 CISP 攻防领域考试中心为维持人员提供咨询及报名申请服务。

- **CISP 攻防领域维持考试流程**

CISP 攻防领域维持考试的流程如下图 2 所示，首先，需要申请资质维持的学员可向所选择的 CISP 攻防领域授权培训机构咨询维持考试申请的相关事宜，然后需按照授权培训机构的指导，提交《CISP 攻防领域续证维持申请表》及其它办理资质维持所需的材料、缴纳维持考试费，报名参加 CISP 攻防领域维持考试，维持考试费由授权培训机构代收。如果所提交材料未达到维持所必须的基本要求，则需要补充材料或等待满足条件后再次申请。提交的各项材料确认无误后，授权培训机构向 CISP 攻防领域考试中心提交维持考生的申请资料及维持考试费，并根据考试中心的统一安排，确定考试时间，并将考试时间通知给学员，在确定的时间内登录 CISP 攻防领域维持考试平台参加考试。如果考试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。

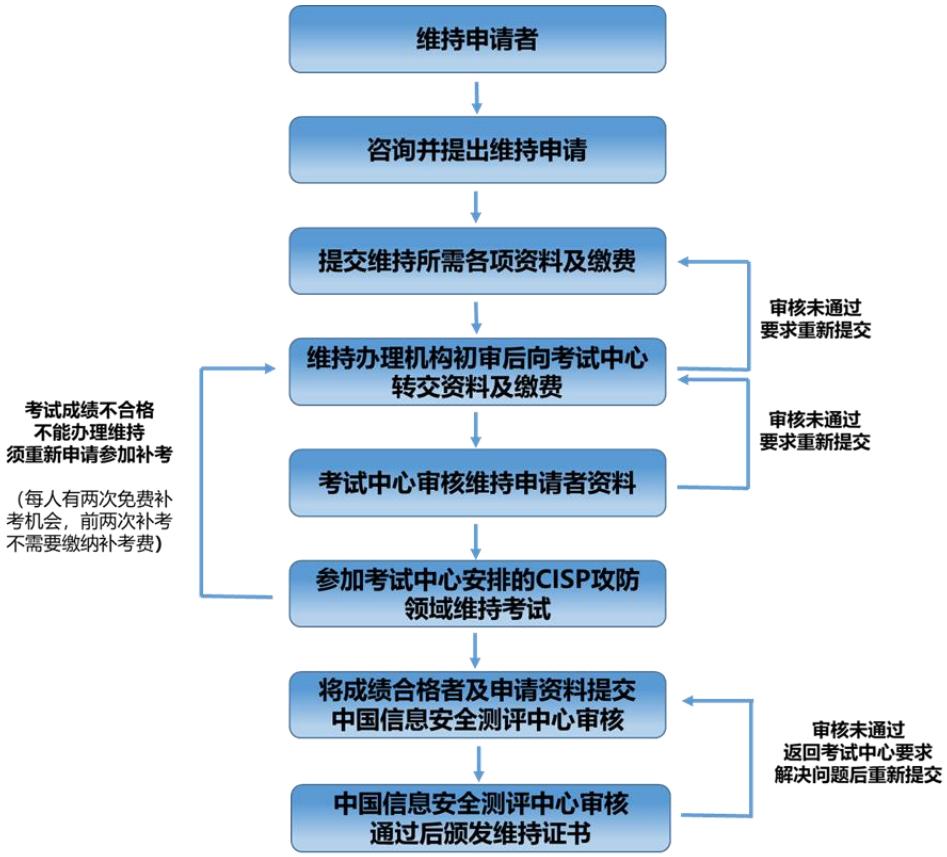



图 2 CISP 攻防领域维持考试流程

考试结束后，CISP 攻防领域考试中心将通过维持考试的维持人员考试成绩及相关材料，统一提交给中国信息安全测评中心进行审核。经审核后，各项条件均通过审核的维持人员，中国信息安全测评中心将为其制作及颁发新的 CISP 攻防领域资质证书。新证书的有效期同样为三年。

## 2、参加 CISP 攻防领域维持考试的要求

- **设备准备**

CISP 攻防领域资质维持考试采用线上双平台同步进行的考试方式，即准备两台终端设备，在考试时分别登录不同的平台共同完成考试与监考工作：

一台电脑：用于通过浏览器登录线上考试地址进行考试。建议使用 Chrome 浏览器访问。

一台监控设备：手机、电脑、平板均可，提前安装“腾讯会议”视频会议应用软件，用于监考。该设备必须保证摄像和语音功能可以正常使用。

以上两部设备，需要参加维持考试的考生提前准备好。

- **考试系统及监考系统**

CISP 攻防领域维持考试，采用专用线上考试系统进行答题，采用腾讯会议进行监控。线上考试系统网址、登录用户名、登录密码、以及腾讯会议 ID 及密码，将在考试前，由各授权培训机构的负责人发放给参考人员。

- **考试环境要求**

考生应选择独立安静房间独自参加考试。整个考试期间，房间必须保持安静明亮，房间内不得有其他人，也不允许出现其他声音。不得由他人替考，也不得接受任何方式助考。

安装“腾讯会议”的设备需放置在考生电脑的侧后边（左/右后侧 45°）。请开启前置摄像头，并确保考生和答题页面能同时收录进屏幕（如下图 3 所示）。

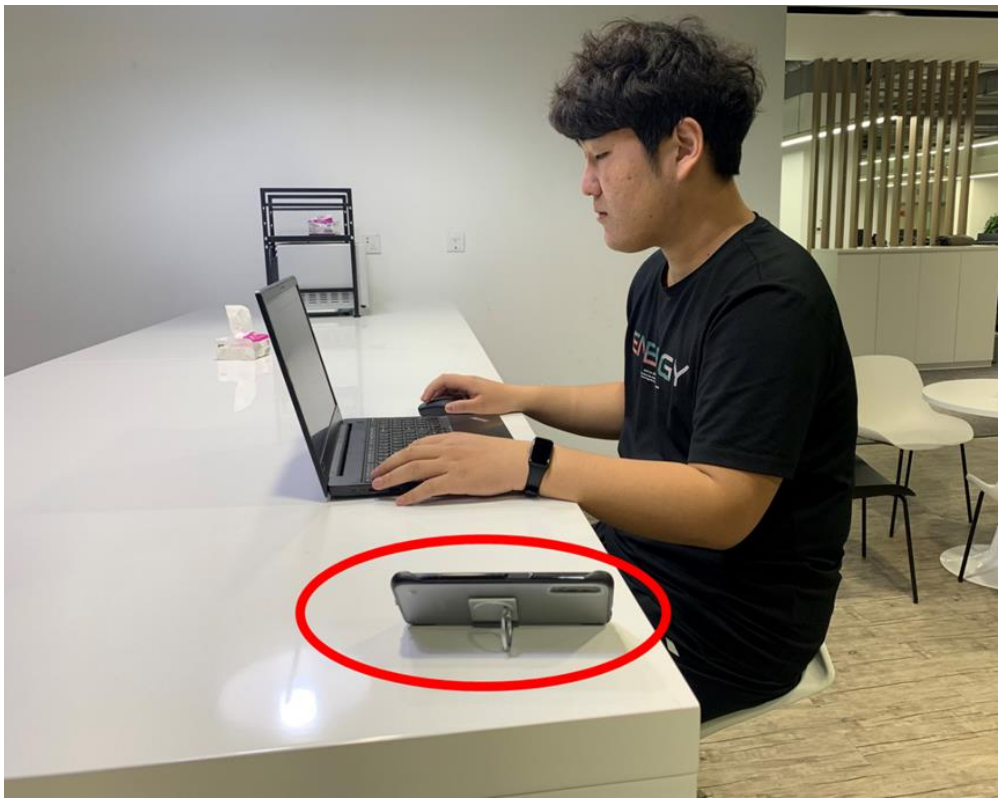


图 3 CISP 维持考试设备摆放方式

- **考试纪律要求**

1）考生须准备好本人身份证，提前 30 分钟进入两个平台，按照监考老师要求， 完成网络设备调试、身份验证核查。

2）开考后，迟到超过 30 分钟及以上登录进入考场者，取消考试资格。

3）考试期间，音频和视频必须全程开启，不得佩戴口罩保证面部清

晰可见，头发不可遮挡耳朵，不得佩戴耳饰。

4) 考试过程中，考生必须保持安静，不得随意起立、走动；不得大声喧哗或引起异常响动扰乱线上考试的考场秩序。

5) 考生应当自觉服从考试工作人员管理，严格遵从考试工作人员关于网络远程考场入场、离场、打开视频，打开考试平台的指令，不得以任何理由妨碍考试工作人员履行职责，不得扰乱网络远程笔试考场的秩序，不得录屏录像录音。

6) 考试过程中应保持网络畅通，如突发网络故障或其他特殊情况，应迅速排除，并及时向监考老师报告，如 5 分钟内没有主动联系监考老师，将视为该考生的考试结束。

7) 考试全程，考生应严格遵守考试纪律。如发现任何违纪行为，将立刻取消该考生的考试资格，并上报中国信息安全测评中心，根据实际的违纪行为严重程度，按照中国信息安全测评中心对违纪人员的相关处理规定进行处理。

## 3、CISP 攻防领域维持考试费用

- **维持考试费**

申请 CISP 攻防领域注册资质维持及报名参加维持考试的人员，应缴纳 CISP 攻防领域注册资质维持考试费。CISP 攻防领域维持考试费金额为 CISP 攻防领域初次考费的 75%。各级别的维持考试费如下：

<table>
<tr><th>维持考试类别</th><th>维持考试费</th><th colspan="2">注册维持考试费组成</th></tr>
<tr><td>CISP-PTE</td><td rowspan="2">3750 元</td><td>注册资质维持考试费</td><td>2250 元</td></tr>
<tr><td>CISP-IRE</td><td>年金（三年）</td><td>1500 元</td></tr>
<tr><td>CISP-PTS</td><td rowspan="2">6000 元</td><td>注册资质维持考试费</td><td>4500 元</td></tr>
<tr><td>CISP-IRS</td><td>年金（三年）</td><td>1500 元</td></tr>
</table>

- **维持考试补考费**

参加 CISP 攻防领域维持考试的人员，每人有两次免费补考机会，如果考生首次维持考试成绩没有通过，后续补考的前两次补考不需要缴纳补考费。如国考生在随后的两次补考中，仍然全部未通过，则从第三次补考开始，考生需要缴纳补考费。补考费为注册资质维持考试费的 50%。各级别的维持考试补考费如下：

| 维持考试补考类别 | 维持考试补考费 |
|---|---|
| CISP-PTE | 1125 元 |
| CISP-IRE | |
| CISP-PTS | 2250 元 |
| CISP-IRS | |

- **超期维持费**

CISP 攻防领域资质证书超期 6 个月以上 10 个月内(含)递交维持申请材料者，除交纳正常维持年金外，还应补交一年维持年金 500 元。证书超期即将届满 1 年，须提前 60 天提出维持换证申请。

# 八、注册信息安全专业人员攻防领域考试中心联系方式

**咨询及索取**

关于 CISP-PTE/CISP-PTS 考试及其维持考试相关的更多信息，请与 CISP 攻防领域考试中心联系。

联系单位：CISP 攻防领域考试中心

【联系地址】北京市西城区西直门外大街 136 号新动力金融科技中心 7 层

【邮政编码】100044

【邮　　箱】CISP@qianxin.com