



**Certified
in Cybersecurity**

ISC2 Certification

认证考试大纲

生效日期: 2025 年 10 月 1 日



ISC2

关于网络安全认证

网络安全认证 (CC) 将向雇主证明您具备入门或初级网络安全职位所需的基础知识、技能和能力。该认证表明您对基本安全最佳实践、政策和程序有一定理解,且愿意并有能力在工作中深入学习,不断成长。

考试涉及五个领域。

- 安全原则
- 业务持续性 (BC)、灾难恢复 (DR) 和应急响应概念
- 访问控制概念
- 网络安全
- 安全运营

经验要求

参加考试没有特定的先决条件。考生应具备基本的信息技术 (IT) 知识。无需网络安全工作经验或任何正规的教育文凭/学位。考生职业生涯的下一步,是获得 ISC2 专家级认证,该认证需要这一领域的工作经验。

认可

CC 符合 ANSI 美国认可委员会 (ANAB) ISO/IEC 标准 17024 的严格要求。

工作任务分析 (JTA)

ISC2 有义务为其成员保持网络安全认证 (CC) 的相关性。定期进行“工作任务分析”(JTA) 是一项有序且关键的流程,旨在确定从事 CC 所定义职业的安全专业人员要执行的任务。JTA 的结果用于更新考试。此流程可确保考生的考试领域与目前信息安全专业从业人员的岗位和职责相关。

网络安全认证 CAT 考试信息

CC 考试的所有英文、简体中文、日文、德文和现代西班牙语考试均采用计算机适应性测试 (CAT)。有关 CC CAT 的更多信息, 请访问 www.isc2.org/certifications/computerized-adaptive-testing。

考试时长	2 小时
题目数量	100 - 125
考试题型	多项选择和高级题型
及格分数	700 分 (满分 1000 分)
考试安排	英语、中文、日语、德语、西班牙语
考试中心	Pearson VUE 考试中心

CC CAT 考试权重

领域	平均权重
1. 安全原则	26%
2. 业务持续性 (BC)、灾难恢复 (DR) 和事故响应概念	10%
3. 访问控制概念	22%
4. 网络安全	24%
5. 安全运营	18%
合计: 100%	



领域 1： 安全原则

1.1 了解信息保障的安全概念

- » 机密性
- » 完整性
- » 可用性
- » 身份验证 (如身份验证方法、多因子验证 (MFA))
- » 不可抵赖性
- » 隐私权

1.2 了解风险管理流程

- » 风险管理 (如风险优先级、风险容忍度)
- » 风险识别、评估和处理

1.3 了解安全控制

- » 技术控制
- » 行政控制
- » 物理控制

1.4 理解 ISC2 道德规范

- » 职业行为准则

1.5 了解治理流程

- » 政策
- » 程序
- » 标准
- » 法律法规



领域 2： 业务持续性 (BC)、灾难恢复 (DR) 和事 故响应概念

2.1 了解业务持续性 (BC)

- » 目的
- » 重要性
- » 构成要素

2.3 了解事故响应

- » 目的
- » 重要性
- » 构成要素

2.2 了解灾难恢复 (DR)

- » 目的
- » 重要性
- » 构成要素



领域 3： 访问控制概念

3.1 了解物理访问控制

- » 物理安全控制 (如胸牌系统、门禁、环境设计)
- » 监控 (如保安、闭路电视 (CCTV)、警报系统、日志等)
- » 授权人员与非授权人员

3.2 了解逻辑访问控制

- » 最小特权原则
- » 职责分离
- » 自主访问控制 (DAC)
- » 强制访问控制 (MAC)
- » 基于角色的访问控制 (RBAC)



领域 4： 网络安全

4.1 了解计算机网络

- » 网络 (如开放系统互连 (OSI) 模型、传输控制协议/互联网协议 (TCP/IP) 模型、互联网协议第 4 版 (IPv4)、互联网协议第 6 版 (IPv6)、WiFi)
- » 端口
- » 应用程序

4.2 了解网络威胁和攻击

- » 威胁类型 (如分布式拒绝服务 (DDoS)、病毒、蠕虫、木马、中间人 (MITM) 攻击、侧信道攻击)
- » 识别 (如入侵检测系统 (IDS)、基于主机的入侵检测系统 (HIDS)、网络入侵检测系统 (NIDS))
- » 防御 (如防病毒、扫描、防火墙、入侵防御系统 (IPS))

4.3 了解网络安全基础设施

- » 内部部署 (如电源、数据中心/机柜、供暖、通风和空调 (HVAC)、环境、灭火、冗余、谅解备忘录 (MOU)/ 协议备忘录 (MOA))
- » 设计 (如网络分段 (隔离区 (DMZ)、虚拟局域网 (VLAN)、虚拟专用网 (VPN)、微分段、纵深防御、网络访问控制 (NAC) (嵌入式系统分段、物联网 (IoT))
- » 云 (如服务等级协议 (SLA)、托管服务提供商 (MSP)、软件即服务 (SaaS)、基础设施即服务 (IaaS)、平台即服务 (PaaS)、混合云)



领域 5： 安全运营

5.1 了解数据安全

- » 加密 (如对称加密、非对称加密、散列加密)
- » 数据处理 (如销毁、保留、分类和标记)
- » 记录和监控安全事件

5.2 了解系统强化

- » 配置管理 (如安全基线、更新、补丁)

5.3 了解安全策略最佳实践

- » 数据处理策略
- » 密码策略
- » 可接受使用策略 (AUP)
- » 自带设备 (BYOD) 策略
- » 变更管理策略 (如归档、审批、回滚)
- » 隐私策略

5.4 了解安全意识培训

- » 目的/概念 (如社会工程学、密码保护)
- » 重要性

其他考试信息

补充参考资料

建议考生通过查阅与 CC 考试大纲相关的专业资料，进一步完善其教育背景与实践经验，并明确需重点加强的学习领域。

如需查看补充参考资料的完整列表，请访问 www.isc2.org/certifications/References。

考试政策和程序

ISC2 建议考生在报名参加考试前，先查看考试政策和程序。请访问 www.isc2.org/Register-for-Exam，全面详细地了解该重要信息。

法律信息

如对 [ISC2 的法律政策](#) 有任何疑问，请发送电子邮件至 legal@isc2.org，与 ISC2 法务部联系。

有任何问题吗？

请联系您所在地区的 ISC2 考生服务部：

美洲

电话：+1-866-331-ISC2 (4722)，按 1
电子邮箱：membersupport@isc2.org

亚太地区

电话：+852-5803-5662
电子邮箱：isc2asia@isc2.org

欧洲、中东和非洲

电话：+44-203-960-7800
电子邮箱：info-emea@isc2.org