Certified in Cybersecurity

ISC2 Certification

认证考试大纲

生效日期:2026 年 9 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
- 安全治理
- 身份与访问管理 (IAM) 概念
- 网络和云安全概念
- 安全操作和事件响应

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 考试的更多信息，请访问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	24%
2、安全治理	17.3%
3、身份与访问管理 (IAM) 概念	20%
4、网络和云安全概念	21.3%
5、安全操作和事件响应	17.3%
	合计：100%

领域 1：安全原则

1.1 了解网络安全概念

» 机密性
» 完整性
» 可用性
» 身份验证、授权、计费（AAA）
» 不可抵赖性
» 隐私权

1.2 了解风险管理概念

» 风险管理生命周期
» 风险管理流程

1.3 了解治理概念

» 法律法规
» 框架和指导方针
» 政策、标准（如国际标准组织 (ISO)、互联网安全中心）、程序

1.4 了解网络安全控制措施

» 技术控制
» 行政控制
» 物理控制

1.5 保持专业和道德操守

» 职业行为准则
» 尽职尽责
» ISC2 道德规范

领域 2：安全治理

2.1 计划治理、风险与合规（GRC）

» 目的
» 重要性
» 框架和工具

2.2 了解冗余

» 业务连续性 (BC)
» 灾难恢复 (DR)

2.3 了解安全意识培训

» 组织文化（如安全的重要性、安全领导力）
» 目的/概念（如社会工程学、密码保护、网络钓鱼）

2.4 衡量网络安全的有效性

» 关键指标、关键风险指标 (KRI)
» 信息表、记分卡、报告

领域 3：身份与访问管理 (IAM) 概念

3.1 了解身份生命周期管理

» 角色定义
» 配置
» 审查
» 取消配置
» 框架和工具

3.2 了解逻辑访问控制

» 最小特权原则 (PoLP)
» 职责分离 (SoD)
» 访问控制模式

领域 4：网络和云安全概念

4.1 了解网络安全

» 概念（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)、虚拟私有网络 (VPN)）
» 防火墙（如端口、应用程序）
» 无线（如 Wi-Fi、蓝牙）
» 嵌入式系统（如工业控制系统 (ICS)）、物联网 (IoT)

4.2 了解网络安全架构

» 理解网络分段（如防火墙区域、虚拟局域网 (VLAN)、微分段）
» 纵深防御
» 零信任 (ZT)

4.3 了解云安全

» 特点（例如，广泛的网络接入、快速弹性、计量服务、按需自助服务、资源池）
» 服务模式
» 部署模式
» 共享安全模式（如角色和责任）

领域 5：
安全操作和事件响应

5.1 了解数据安全

» 数据处理（如分类、标记、屏蔽和脱敏）
» 加密（如对称、非对称、散列、量子抗性密码学）

5.2 了解安全操作

» 记录和监控安全事件
» 安全事件分流（如事件用例、优先级排序、相关性）
» 威胁行为者（如类型、动机）
» 网络威胁情报
» 威胁框架

5.3 了解事件响应 (IR)

» 实施事件响应计划 (IRP) 的数据处理政策
» 事件响应 (IR) 演练（如测试、桌面演习）

5.4 了解资产保护

» 资产生命周期管理（如软件和设备的使用生命终止 (EOL)）
» 配置和变更管理

5.5 了解安全测试

» 安全就绪测试（如蓝色团队、紫色团队、红色团队）
» 应用程序测试（如漏洞扫描、静态分析、动态分析、威胁建模）
» 物理渗透测试（如网络钓鱼、尾随、假冒等）

其他考试信息

补充参考资料

我们建议考生查阅与 CC 考试大纲相关的专业资料，并明确需重点加强的学习领域，以进一步完善自己的教育背景与实践经验。

如需查看补充参考资料的完整列表，请访问 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 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