CC SM

Certified in Cybersecurity

An (ISC)² Certification

认证考试大纲

生效日期：2022 年 8 月 29 日

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

关于网络安全认证

网络安全认证 (CC) 向雇主证明您具备 网络安全 入门或初级职位所需的基本知识、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，并且您愿意且有能力在工作中深入学习，得到成长。

考试涉及五个领域:

- 安全原则
- 业务连续性 (BC)、灾难恢复 (DR) 和事故响应概念
- 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。没有网络安全工作经验或任何正式的教育文凭/学位要求。考生职业生涯的下一步将敦促其获得 (ISC)² 专家级认证，因而需要该领域的经验。

工作任务分析 (JTA)

(ISC)² 有义务保持其会员所持 CC 认证的相关性。定期进行工作任务分析（JTA）是一项系统而关键的过程，用以确定 安全专业人士 从事 CC 所定义的专业领域所执行的任务。JTA 的分析结果会用来更新考试。此过程确保考生的测试题目与目前从业的信息安全专业人士的角色和职责密切相关。

CC 考试信息

考试时长	2 小时
考题数量	100
考题类型	多选题
及格分数	1000 分获得 700 分
考试语言	英语，日语，中文，韩语，德语，西班牙语
考试中心	Pearson VUE Testing Center

CC 考试的权重

领域	平均权重
1.安全原则	26%
2.业务连续性 (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%
总计:	**100%**

领域 1:
安全原则

1.1 了解信息保障的安全概念

» 保密性
» 完整性
» 可用性
» 身份验证（例如，验证方法、多因子验证(MFA)）
» 不可抵赖性
» 隐私性

1.2 了解风险管理流程

» 风险管理(例如，风险优先级、风险承受能力)
» 风险识别、评估和处理

1.3 了解安全概念

» 技术控制 措施
» 行政控制 措施
» 物理控制 措施

1.4 了解 (ISC)² 道德规范

» 职业行为准则

1.5 了解治理过程

» 策略
» 程序
» 标准
» 法律法规

领域 2:
业务连续性 (BC)、灾难恢复 (DR) 和事故响应概念

2.1 了解业务连续性 (BC)

» 目的
» 重要性
» 组成部分

2.2 了解灾难恢复 (DR)

» 目的
» 重要性
» 组成部分

2.3 了解事故响应

» 目的
» 重要性
» 组成部分

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 措施 （例如，胸牌系统、大门入口、环境设计）
» 监控（如保安、闭路电视 (CCTV)、报警系统、日志）
» 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（例如，开放系统互连 (OSI) 模型、传输控制协议/互联网协议 (TCP/IP) 模型、互联网协议版本 4 (IPv4)、互联网协议版本 6 (IPv6)、WiFi）
» 端口
» 应用

4.2 了解网络威胁和攻击

» 威胁类型（例如，分布式拒绝服务 (DDoS)、病毒、蠕虫、木马、中间人 (MITM)、旁路）
» 识别（例如，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（例如，防病毒、扫描、防火墙、入侵防御系统 (IPS)）

4.3 了解网络安全基础架构

» 内部部署（例如，电源、数据中心/数据室、采暖、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（例如，网络分段（非军事区 (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)（嵌入式系统的分段、物联网 (IoT)）
» 云（例如，服务等级协议 (SLA)、管理服务提供商 (MSP)、软件即服务 (SaaS)、基础架构即服务 (IaaS)、平台即服务 (PaaS)、混合）

领域 5:
安全运营

5.1 了解数据安全

» 加密（例如，对称、非对称、散列）
» 数据处理（例如，销毁、保留、分类、标记）
» 记录和监控安全事件

5.2 了解系统强化

» 配置管理（例如，基线、更新、补丁）

5.3 了解最佳实践安全政策

» 数据处理政策
» 密码政策
» 可接受使用政策 (AUP)
» 自带设备 (BYOD) 政策
» 变更管理政策（例如，归档、批准、回滚）
» 隐私政策

5.4 了解安全意识培训

» 目的/概念（例如，社会工程、密码保护）
» 重要性

额外考试信息

考试政策和程序

(ISC)² 建议网络安全认证考生在报名参加考试之前查看考试政策和程序。请访问 www.isc2.org/Register-for-Exam 阅读此重要信息的详细解释。

法律信息

如对 (ISC)² 的法律政策有任何问题，
请联系 (ISC)² 法务部（电子邮件：legal@isc2.org）。

有任何问题?

联系您所在地区的(ISC)² 考生服务：

美洲

电话：+1-866-331-ISC2 (4722)
电子邮件：info@isc2.org

亚太地区

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

欧洲、中东和非洲

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