



**Certified
in Cybersecurity**

ISC2 Certification

认证考试大纲

生效日期:2022年8月29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，并且您愿意且有能力在工作中进行深入学习，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。

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) 是一项有序而关键的过程，旨在确定从事 CC 所定义职业的安全专业人员所执行的任务。JTA 的分析结果会用来更新本考试。此过程可确保考生的测试主题领域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
题目数量	100
考试题型	选择题
及格分数	700 分（满分 1000 分）
考试语言	英语、中文、日语、德语
考试中心	Pearson VUE 考试中心

CC 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) 和应急响应概念	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 了解信息保证的安全概念

- » 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

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 了解 (ISC)² 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
- » 组成部分

2.3 了解事故响应

- » 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



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、大门入口、环境设计）
- » 监控（如保安、闭路电视监控系统 (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（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（例如，分布式拒绝服务 (DDoS)、病毒、蠕虫、木马、中间人攻击 (MITM)、侧信道)
- » 身份识别（例如，入侵侦测系统 (IDS)、基于主机的入侵检测系统 (HIDS)、网络入侵检测系统 (NIDS)
- » 预防（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、供暖、通风与空调 (HVAC)、环境、灭火、冗余、理解备忘录 (MOU)/协议备忘录 (MOA)
- » 设计（如网络分段（非军事区 (DMZ)、虚拟局域网 (VLAN)、虚拟私有网络 (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（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 了解系统安全强化

- » 配置管理（如安全基线、更新、补丁等）

5.3 了解安全政策最佳实践

- » 数据处理政策
- » 密码政策
- » 可接受使用原则 (AUP)
- » 自带设备 (BYOD) 政策
- » 变更管理政策（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（如社会工程学、密码保护）
- » 重要性

其他考试信息

考试政策和程序

ISC2 建议考生在报名参加考试前查看考试政策和程序。请在以下网站阅读此重要信息的详细解释：www.isc2.org/Register-for-Exam。

法律信息

如对 [ISC2 的法律政策](#) 有任何问题，请联系 ISC2 法务部：legal@isc2.org。

有任何问题吗？

请联系您所在地区的 ISC2 考生服务部门：

美洲

电话：+1-866-331-ISC2 (4722)

电子邮件：membersupport@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