CISSP®

Certified Information Systems Security Professional

ISC2 Certification

认证考试大纲

生效日期:2024 年 4 月 15 日

ISC2™

关于 CISSP

信息系统安全认证专家 (CISSP) 是信息安全市场中全球认可度最高的认证。CISSP 认证证明信息安全专业人员拥有深厚的技术和管理知识与经验，能够有效地设计和管理组织的整体安全状况。

CISSP 知识体系中所包含的广泛主题确保了其在信息安全领域所有学科中的相关性。考试合格的考生能够胜任以下八个领域的工作：

- 安全与风险管理
- 资产安全
- 安全架构和工程设计
- 通信和网络安全
- 身份识别访问管理 (IAM)
- 安全评估和测试
- 安全运营
- 软件开发安全

经验要求

考生必须在现行《CISSP 考试大纲》八个领域中的两个或以上领域累计有至少五年的全职工作经验。如果拥有计算机科学、IT 或相关领域的学士学位或更高的学位，或者拥有 ISC2 批准的清单中的其他认证证书， 可满足一年的工作经验要求。兼职工作或实习经验也可计入工作经验要求。

不具备 CISSP 所需经验的考生，可在通过 CISSP 考试后成为 ISC2 准会员。然后，ISC2 准会员将有六年的时间来获得所需的五年经验。您可以在以下网站了解有关 CISSP 的经验要求，以及如何计算兼职工作和实习经验的更多信息：www.isc2.org/Certifications/CISSP/experience-requirements。

认证

CISSP 是信息安全领域第一个符合 ANSI/ISO/IEC 标准 17024 严格要求的证书。

工作任务分析 (JTA)

ISC2 有义务为其成员保持 CISSP 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 CISSP 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。

CISSP CAT 考试信息

CISSP 考试对所有英语、德语、现代西班牙语、日语和简体中文考试采用计算机自适应测试 (CAT)。有关 CISSP CAT 的更多信息，请访问 www.isc2.org/certificatons/CISSP-CAT。

考试时长	3 小时
题目数量	100 - 150
考试题型	选择题和高级创新题目
及格分数	700 分（满分 1000 分）
考试语言	中文、英语、德语、日语、西班牙语
考试中心	ISC2 授权 PPC 和 PVTC 定点 Pearson VUE 考试中心

CISSP CAT 考试权重

领域	平均权重
1. 安全与风险管理	16%
2. 资产安全	10%
3. 安全架构和工程设计	13%
4. 通信和网络安全	13%
5. 身份识别访问管理 (IAM)	13%
6. 安全评估和测试	12%
7. 安全运营	13%
8. 软件开发安全	10%
总计：	**100%**

领域 1：安全与风险管理

1.1 理解、遵守并促进职业道德

» ISC2 职业道德规范
» 组织道德规范

1.2 理解并应用安全概念

» 机密性、完整性和可用性、真实性与不可抵赖性（信息安全的 5 大支柱）

1.3 评估和应用安全治理原则

» 根据业务战略、目标、任务和目的调整安全职能
» 组织流程（如收购、资产剥离、治理委员会）
» 组织角色和责任
» 安全控制框架（例如，国际标准组织 (ISO)、国家标准与技术协会 (NIST)、信息和相关技术控制目标 (COBIT)、Sherwood 业务安全架构 (SABSA)、支付卡行业 (PCI)、联邦风险和授权管理计划 (FedRAMP)）
» 尽职调查

1.4 全面了解与信息安全相关的法律法规事项

» 网络犯罪和数据泄露
» 许可与知识产权要求
» 进出口控制
» 跨境数据流
» 与隐私相关的问题（例如，《一般数据保护条例》(GDPR)、《加州消费者隐私法案》、中国《个人信息保护法》、南非《个人信息保护法》）
» 合同、法律、行业标准和监管要求

1.5 了解调查类型（即行政、刑事、民事、监管、行业标准）的要求

1.6 制定、记录和实施安全政策、标准、程序和指南

1.7 确定、分析、评估和实现业务持续性 (BC) 要求并确定优先次序

» 业务影响分析 (BIA)
» 外部依赖

1.8 促成并执行人员安全方面的政策和程序

- 应聘者筛选与聘用
- 雇佣协议和政策驱动的要求
- 入职、调动和终止流程
- 供应商、顾问和承包商协议及控制措施

1.9 理解并应用风险管理概念

- 威胁和漏洞识别
- 风险分析、评估和范围
- 风险响应和处理（如网络安全保险）
- 适用的控制类型（如预防性、侦查性、纠正性）
- 控制评估（如安全和隐私）
- 持续监控和测量
- 报告（如内部和外部）
- 持续改进（如风险成熟度建模）
- 风险框架（例如，国际标准组织 (ISO)、国家标准与技术协会 (NIST)、信息和相关技术控制目标 (COBIT)，Sherwood 业务安全架构 (SABSA)、支付卡行业 (PCI)）

1.10 理解并应用威胁建模的概念和方法

1.11 应用供应链风险管理 (SCRM) 概念

- 与从供应商和提供商采购产品和服务相关的风险（例如，产品篡改、仿冒品、植入物）
- 风险缓解措施（例如，第三方评估和监控、最低安全要求、服务等级要求、硅信任根、物理不可克隆功能、软件物料清单）

1.12 建立并维护安全意识、教育和培训计划

- 加强意识和增加培训的方法与技巧（例如社会工程、网络钓鱼、安全冠军、游戏化）
- 定期审查内容，包括新兴技术和趋势（例如，加密货币、人工智能（AI）、区块链）
- 评估计划成效

领域 2：资产安全

2.1 对信息和资产进行识别和分类

» 数据分类
» 资产分类

2.2 制定信息和资产处理要求

2.3 安全地提供信息和资产

» 信息和资产所有权
» 资产库存（如有形资产、无形资产）
» 资产管理

2.4 管理数据生命周期

» 数据角色（即所有者、控制者、保管者、处理者、用户/主体）
» 数据收集
» 数据位置
» 数据维护
» 数据保留
» 数据恢复
» 数据销毁

2.5 确保适当的资产保留（如使用寿命结束 (EOL)、支持终止 (EOS)）

2.6 确定数据安全控制与合规要求

» 数据状态（如使用中、传输中、静态）
» 范围界定和定制
» 标准选择
» 数据保护方法（如数字化权限管理 (DRM)、数据丢失防护 (DLP)、云访问安全代理 (CASB)）

领域 3：安全架构和工程设计

3.1 利用安全设计原则来研究、实施和管理工程流程

- 威胁建模
- 最小特权
- 纵深防御
- 安全默认设置
- 安全失效
- 职责分离 (SoD)
- 保持简单小巧
- 零信任或信任但验证
- 隐私设计
- 责任共担
- 安全访问服务边缘

3.2 了解安全模型的基本概念（如 Biba 模型、星形模型、Bell-LaPadula 模型等）

3.3 根据系统安全需求选择控制措施

3.4 了解信息系统 (IS) 的安全功能（例如内存保护、可信赖平台模块 (TPM)、加密/解密）

3.5 评估并缓解安全架构、设计和解决方案组件的漏洞

- 客户端系统
- 服务器端系统
- 数据库系统
- 加密系统
- 工业控制系统 (ICS)
- 基于云的系统（如软件即服务 (SaaS)、基础架构即服务 (IaaS)、平台即服务 (PaaS)）
- 分布式系统
- 物联网 (IoT)
- 微服务（例如，应用编程接口(API)）
- 容器化
- 无服务器计算
- 嵌入式系统
- 高性能计算 (HPC) 系统
- 边缘计算系统
- 虚拟化系统

3.6 选择和确定加密解决方案

- 密码生命周期（如密钥、算法选择）
- 加密方法（如对称、非对称、椭圆曲线、量子等）
- 公钥基础架构 (PKI)（例如，量子密钥分配）
- 密钥管理实践（例如，轮换）
- 数字签名和数字证书（例如，不可抵赖性、完整性）

3.7 了解密码分析攻击的方法

- 蛮力
- 唯密文攻击
- 已知明文攻击
- 频率分析
- 选择密文攻击
- 实现攻击
- 侧信道
- 故障注入
- 时序攻击
- 中间人攻击 (MITM)
- 哈希传递
- Kerberos 漏洞利用
- 勒索软件攻击

3.8 在场地和设施的设计中应用安全原则

3.9 设计场地和设施安全控制

- 配线柜/中间配线设施
- 服务器机房/数据中心
- 媒体存储设施
- 证据存储
- 限制区和工作区安全
- 公用事业和供暖、通风与空调 (HVAC)
- 环境问题（例如，自然灾害，人为造成的问题）
- 火灾预防、探测和扑灭
- 电源（如冗余、备用电源）

3.10 管理信息系统生命周期

- 利益相关者的需求和要求
- 需求分析
- 体系结构设计
- 开发/实现
- 集成
- 核查与验证
- 过渡/部署
- 操作和维护/维持
- 退役/处置

领域 4：通信和网络安全

4.1 在网络架构中应用安全设计原则

» 开放系统互连 (OSI) 和传输控制协议/互联网协议 (TCP/IP) 模型
» 互联网协议 (IP) 版本 4 和 6 (IPv6)（例如，单播、广播、多播、任播）
» 安全协议（例如，互联网协议安全 (IPSec)、SSH、安全套接层 (SSL)/传输层安全 (TLS)）
» 多层协议的含义
» 融合协议（例如，互联网小型计算机系统接口 (iSCSI)、IP 语音 (VoIP)、InfiniBand over Ethernet (IBoE)、计算快速链接 (CEL)）
» 传输架构（例如，拓扑、数据/控制/管理平面、直通/存储转发）
» 性能指标（例如，带宽、延迟、抖动、吞吐量、信噪比）
» 流量（例如，南北、东西向）
» 物理分段（例如，带内、带外、气隙）
» 逻辑分段（例如，虚拟局域网（VLAN）、虚拟私有网络（VPN）、虚拟路由转发、虚拟域）
» 微分段（例如，网络覆盖/封装；分布式防火墙、路由器、入侵侦测系统 (IDS)/入侵防御系统 (IPS)、零信任）
» 边缘网络（例如，入口/出口、对等互连）
» 无线网络（例如，蓝牙、Wi-Fi、Zigbee、卫星）
» 蜂窝/移动网络（例如，4G、5G）
» 内容分发网络 (CDN)
» 软件定义网络 (SDN)（例如，应用编程接口 (API)、软件定义广域网、网络功能虚拟化）
» 虚拟专有云 (VPC)
» 监控和管理（例如，网络可观测性、流量/整形、容量管理、故障检测和处理）

4.2 安全网络组件

» 基础设施运行（如冗余电源、保修、支持）
» 传输介质（例如，介质的物理安全性、信号传播质量）
» 网络访问控制 (NAC) 系统（例如，物理和虚拟解决方案）
» 端点安全（例如，基于主机）

4.3 根据设计实现安全通信渠道

» 语音、视频和协作（例如会议、Zoom 房间）
» 远程访问（例如，网络管理功能）
» 数据通信（例如，回程网络、卫星）
» 第三方连接（例如，电信提供商、硬件支持）

领域 5：身份识别访问管理 (IAM)

5.1 控制资产的物理和逻辑访问

- 信息
- 系统
- 设备
- 设施
- 应用程序
- 服务

5.2 设计识别和身份验证策略（例如，人员、设备和服务）

- 群组和角色
- 验证、授权和审计 (AAA)（例如，多因子验证 (MFA)、无密码身份验证）
- 会话管理
- 身份登记、证明和确定
- 联合身份管理 (FIM)
- 凭证管理系统（如密码保管库）
- 单点登录 (SSO)
- 准时生产

5.3 与第三方服务的联合身份

- 本地
- 云
- 混合

5.4 实现和管理授权机制

- 基于角色的访问控制 (RBAC)
- 基于规则的访问控制
- 强制访问控制 (MAC)
- 自主访问控制 (DAC)
- 基于属性的访问控制 (ABAC)
- 基于风险的访问控制
- 访问策略执行（例如，策略决策点、策略执行点）

5.5 管理身份和访问配置生命周期

- 账户访问审查（如用户、系统、服务）
- 置备和取消置备（如入职/离职和调动）
- 服务账户管理
- 角色定义和转换（例如，分配到新角色的人员）
- 特权升级（例如，使用 sudo，审核其使用）

5.6 实现身份验证系统

领域 6：安全评估和测试

6.1 设计并验证评估、测试及审计策略

- 内部（例如，在组织控制范围内）
- 外部（例如，在组织控制范围外）
- 第三方（例如，在企业控制范围外）
- 位置（例如，本地、云、混合）

6.2 进行安全控制测试

- 漏洞评估
- 渗透测试（例如，红队、蓝队和/或紫队演练）
- 日志审核
- 综合事务/基准
- 代码审查和测试
- 滥用案例测试
- 覆盖率分析
- 接口测试（例如用户界面、网络接口、应用编程接口(API)）
- 入侵攻击模拟
- 合规检查

6.3 收集安全流程数据(如技术和管理数据)

- 账户管理
- 管理审查和批准
- 关键绩效和风险指标
- 备份验证数据
- 培训和意识
- 灾难恢复（DR）和业务持续性（BC）

6.4 分析测试输出并生成报告

- 补救
- 异常处理
- 道德披露

6.5 开展或协调安全审计

- 内部（例如，在组织控制范围内）
- 外部（例如，在组织控制范围外）
- 第三方（例如，在企业控制范围外）
- 位置（例如，本地、云、混合）

领域 7：安全运营

7.1 了解并配合调查

- 证据收集和处理
- 报告和文档
- 调查技巧
- 数字取证工具、策略和程序
- 工件（如计算机、网络、移动设备）

7.2 开展记录和监控活动

- 入侵检测和预防 (IDPS)
- 安全信息与事件管理 (SIEM)
- 持续监控和调优
- 出站监控
- 日志管理
- 威胁情报（如威胁情报源、威胁狩猎）
- 用户和实体行为分析 (UEBA)

7.3 执行配置管理 (CM)（如置备、基线确定、自动化）

7.4 应用基础安全运营概念

- 按需知密/最小特权
- 职责分离 (SoD) 和责任
- 特权账户管理
- 工作轮换
- 服务等级协议 (SLA)

7.5 应用资源保护

- 介质管理
- 介质保护技术
- 静止数据/传输中数据

7.6 执行事件管理

- 检测
- 响应
- 缓解
- 报告
- 恢复
- 补救
- 经验教训

7.7 运行和维护检测和预防措施

- 防火墙（如下一代防火墙、网端应用防火墙、网络防火墙）
- 入侵侦测系统 (IDS) 和入侵防御系统 (IPS)
- 白名单/黑名单
- 第三方提供的安全服务
- 沙盒化
- 蜜罐/蜜网
- 反恶意软件
- 基于机器学习和人工智能 (AI) 的工具

7.8 实施并支持补丁和漏洞管理

7.9 了解并参与变更管理流程

7.10 实施恢复策略

- 备份存储策略（例如，云存储、现场、异地）
- 恢复站点策略（例如，冷站点与热站点、资源能力协议）
- 多个处理站点
- 系统弹性、高可用性 (HA)、服务质量 (QoS) 和容错

7.11 实施灾难恢复 (DR) 流程

- 响应
- 个人
- 通信（如方法）
- 评估
- 复原
- 培训和意识
- 经验教训

7.12 测试灾难恢复计划 (DRP)

- 通读/桌面
- 演练
- 模拟
- 平行
- 完全中断
- 通信（如利益相关者、测试状态、监管机构）

7.13 参与业务持续性 (BC) 规划和演习

7.14 实现和管理物理安全

- 边界安全控制
- 内部安全控制

7.15 解决人员安全和安保问题

- 旅行
- 安全培训和安全意识（例如，内部威胁、社交媒体影响、双因子验证 (2FA) 疲劳攻击）
- 紧急情况管理
- 胁迫

领域 8：软件开发安全

8.1 了解软件开发生命周期 (SDLC) 中的安全并将其融入其中

- 开发方法（例如，敏捷、瀑布式、DevOps、DevSecOps、扩展敏捷框架）
- 成熟度模型（例如，能力成熟度模型 (CMM)、软件保障成熟度模型 (SAMM)）
- 操作和维护
- 变更管理
- 综合产品团队

8.2 在软件开发生态系统中识别和应用安全控制

- 编程语言
- 库
- 工具套件
- 集成开发环境
- 运行时
- 持续集成和持续交付 (CI/CD)
- 软件配置管理 (CM)
- 代码库
- 应用程序安全测试（例如，静态应用程序安全测试 (SAST)、动态应用程序安全测试 (DAST)、软件组成分析、交互式应用安全测试 (IAST)）

8.3 评估软件安全的有效性

- 变更审计和记录
- 风险分析与缓解

8.4 评估所获软件的安全影响

- 商用现货 (COTS)
- 开源
- 第三方
- 托管服务（例如，企业应用程序）
- 云服务（例如，软件即服务 (SaaS)、基础架构即服务 (IaaS)、平台即服务 (PaaS)）

8.5 定义并应用安全编码指南和标准

- 源代码层面的安全弱点和漏洞
- 应用编程接口 (API) 安全
- 安全编码实践
- 软件定义的安全

附加考试信息

补充参考

我们鼓励考生通过查阅与 CBK 相关的资源来补充自己的教育和经验，并确定可能需要额外关注的学习领域。

要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 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)，并按 1
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 (0)203-960-7800
电子邮件：info-emea@isc2.org