CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

认证考试大纲

生效日期：2021 年 5 月 1 日

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

关于 CISSP

信息系统安全认证专家 (CISSP) 是信息安全领域最被全球广泛认可的认证。CISSP 认证反映了持证者具备有效设计、构建及管理组织整体安全态势所需的深厚信息安全技术、管理知识、技能与经验。

CISSP 公共知识体系 (CBK®) 中包含的广泛议题确保了与信息安全领域所有原理的相关性。通过认证的考生展示了在以下八大知识域的能力：

- 安全与风险管理
- 资产安全
- 安全架构与工程
- 通信与网络安全
- 身份识别访问管理
- 安全评估与测试
- 安全运营
- 软件开发安全

经验要求

考生必须在 CISSP 公共知识体系 (CBK) 八大知识域中的至少两个或两个以上领域，拥有至少 5 年全职工作经验。拥有 4 年大学本科学历或同等学历，或者 (ISC)² 认可的其它证书可以抵免一年的工作经验。所有教育学位最多只能抵免一年工作经验。

没有满足 CISSP 所需工作经验的考生，如果能够通过 CISSP 考试则可以成为 (ISC)² 的准会员(即 Associate) 。(ISC)² 的准会员可以用接下来的 6 年时间积累所需的五年工作经验。欲了解更多关于 CISSP 工作经验要求以及如何计算兼职工作和实习经验的信息，请访问 www.isc2.org/Certifications/CISSP/experience-requirements。

认证

CISSP 是业界首张符合 ANSI/ ISO/IEC 17024 国际标准严格要求的信息安全认证。

工作任务分析 (JTA)

(ISC)² 有义务保持其会员所持 CISSP 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，用以确定从事 CISSP 所定义专业领域的安全专业人士所执行的任务。JTA 的分析结果会用来更新考试。此过程确保了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。

CISSP 计算机自适应测试 (CAT) 考试信息

CISSP 的所有英语考试都采用计算机自适应测试 (CAT) 。CISSP 的其它语种考试采用线性和固定格式的测试。欲了解 CISSP 的 CAT 详情，请访问 www.isc2.org/certificatons/CISSP-CAT。

考试时长	3 小时
考题数量	100 - 150
考题格式	多项选择和高级创新型考题
及格分数	700（满分 1000）
可提供的考试语言	英语
测试中心	(ISC)² 授权且由 PPC 和 PVTC 精选的 Pearson VUE 测试中心

CISSP CAT 考试的权重

领域	平均权重
1.安全与风险管理	15%
2.资产安全	10%
3.安全架构与工程	13%
4.通信与网络安全	13%
5.身份识别访问管理	13%
6.安全评估与测试	12%
7.安全运营	13%
8.软件开发安全	11%
总计：	**100%**

CISSP 线性考试信息

考试时长	6 小时
考题数量	250
考题格式	多项选择和高级创新型考题
及格分数	700（满分 1000）
可提供的考试语言	法语、德语、巴西葡萄牙语、现代西班牙语、日语、简体中文、韩语
测试中心	(ISC)²授权且由 PPC 和 PVTC 精选的 Pearson VUE 测试中心

CISSP 线性考试权重

领域	权重
1.安全与风险管理	15%
2.资产安全	10%
3.安全架构与工程	13%
4.通信与网络安全	13%
5.身份识别访问管理	13%
6.安全评估与测试	12%
7.安全运营	13%
8.软件开发安全	11%
总计：	**100%**

领域 1：安全与风险管理

1.1 理解、遵从与提升职业道德

» (ISC)² 职业道德规范
» 组织的道德规范

1.2 理解和应用安全概念

» 保密性、完整性、可用性、真实性和不可否认性

1.3 评估和应用安全治理的原理

» 将安全功能与业务战略、目标、使命和宗旨相关联
» 组织过程（例如，收购、剥离、治理委员会）
» 组织角色和职责
» 安全控制框架
» 谨慎考虑/恪尽职守

1.4 确定合规性和其他要求

» 合约、法律、行业标准和监管要求
» 隐私要求

1.5 理解在全球背景下与信息安全相关的法律和监管问题

» 网络犯罪和数据泄露
» 许可和知识产权 (IP) 要求
» 进口/出口控制
» 跨境数据流
» 隐私

1.6 理解调查类型的要求（即行政、刑事、民事、监管、行业标准）

1.7 制定、记录和实施安全政策、标准、程序和指南

1.8 对业务连续性 (BC) 要求进行识别、分析及优先级排序

- 业务影响分析 (BIA)
- 制定和记录范围和计划

1.9 协助制定和实施人员安全政策和程序

- 员工筛选与雇佣
- 雇佣协议与政策
- 员工入职、调动和离职流程
- 供应商、顾问与承包商协议与控制
- 合规策略要求
- 隐私策略要求

1.10 理解并应用风险管理概念

- 识别风险与漏洞
- 风险评估/分析
- 风险响应
- 对策选择与实施
- 适用的控制类型（如预防、检测、纠正）
- 控制评估（安全与隐私）
- 监控与测量
- 报告
- 持续提高（如风险成熟度模型）
- 风险框架

1.11 理解并应用威胁建模的概念和方法

1.12 应用供应链风险管理 (SCRM) 概念

- 与硬件、软件和服务相关的风险
- 第三方评估和监控
- 最低安全要求
- 服务水平要求

1.13 制定并维护安全意识、教育和培训计划

- 安全意识宣贯与培训的方法和技术（例如，社会工程、网络钓鱼、安全冠军、游戏化）
- 定期内容审查
- 方案效果评估

领域 2：资产安全

2.1 识别并分类信息和资产

» 数据分类
» 资产分类

2.2 制定信息和资产处理要求

2.3 安全配置资源

» 信息和资产所有权
» 资产列表（如有形、无形）
» 资产管理

2.4 管理数据生命周期

» 数据角色（例如，所有者、控制者、保管员、处理员、用户/对象）
» 数据采集
» 数据位置
» 数据维护
» 数据保留
» 数据残留
» 数据销毁

2.5 确保适当的资产保留（例如，使用寿命结束 (EOL)，支持结束 (EOS)）

2.6 确定数据安全控制和合规要求

» 数据状态（例如，使用中、传输中、静止）
» 数据定界和定制
» 标准选择
» 数据保护方法（例如，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：安全架构与工程

3.1 使用安全设计原理来研究、实施与管理工程过程

- 威胁建模
- 最小权限
- 深度防御
- 默认安全配置
- 失效安全
- 职责分离 (SoD)
- 保持简单
- 零信任
- 通过设计保护隐私
- 信任但要确认
- 共同责任

3.2 理解安全模型的基本概念（例如 Biba、Star Model、Bell-LaPadula 等模型）

3.3 基于系统安全要求选择控制措施

3.4 理解信息系统 (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 评估并降低安全架构、设计和解决方案方面的漏洞

- 基于客户端的系统
- 基于服务器的系统
- 数据库系统
- 密码系统
- 工业控制系统 (ICS)
- 基于云端的系统（例如，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
- 容器化
- 无服务器
- 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（例如：对称、非对称、椭圆曲线、量子）
- 公钥基础架构 (PKI)
- 密钥管理实践
- 数字签名和数字证书
- 不可否认性
- 完整性（例如：哈希函数）

3.7 理解密码分析攻击方法

- 暴力破解
- 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
- 边信道
- 故障注入
- 定时
- 中间人攻击 (MITM)
- 哈希传递攻击
- Kerberos 协议攻击
- 勒索软件

3.8 将安全原理运用到场所与设施的设计上

3.9 设计场所和设施安全控制措施

- 配线柜/中继配电设施
- 服务器机房/数据中心
- 媒体储存设施
- 证据储存
- 限制区与工作区的安全
- 公用事业设备及供暖、通风与空调 (HVAC)
- 环境问题
- 防火、检测和灭火
- 电源（如冗余、备份）

领域 4：通信与网络安全

4.1 评估和实施网络架构中的安全设计原则

» 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) 网络（例如，互联网协议安全 (IPSec)、互联网协议 (IP) v4/6)
» 安全协议
» 多层协议的含义
» 聚合协议（例如，以太网光纤通道 (FCoE)、互联网小型计算机系统接口 (iSCSI)、IP 语音 (VoIP))
» 微隔离（例如，软件定义网络 (SDN)、虚拟可扩展局域网 (VXLAN)、封装、软件定义广域网 (SD-WAN))
» 无线网络（如 Li-Fi、Wi-Fi、Zigbee、卫星）
» 蜂窝网络（如 4G、5G)
» 内容分发网络 (CDN)

4.2 安全的网络组件

» 硬件操作（例如，冗余电源、保修、支持）
» 传输媒介
» 网络访问控制 (NAC) 设备
» 终端安全

4.3 根据设计实施安全通信通道

» 语音
» 多媒体协同
» 远程访问
» 数据通信
» 虚拟网络
» 第三方连接

领域 5：
身份识别访问管理

5.1 控制对资产的物理和逻辑访问

- 信息
- 系统
- 设备
- 设施
- 应用程序

5.2 管理对人员、设备和服务的身份认证与验证

- 实施施身份管理 (IdM)
- 单/多因子验证 (MFA)
- 可核查性
- 会话管理
- 身份注册、证明和建立
- 联合身份管理 (FIM)
- 凭证管理系统
- 单点登录 (SSO)
- 准时生产 (JIT)

5.3 通过第三方服务进行联合身份验证

- 本地部署
- 云端
- 混合

5.4 实施和管理授权机制

- 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

5.5 管理身份和访问配置生命周期

- 帐户访问审查（如用户、系统、服务）
- 预配和取消预配（如入职、离职和调动）
- 角色定义（例如，分配到新角色的人员）
- 特权升级（例如，托管服务帐户、使用 sudo、最小化其使用）

5.6 部署身份验证系统

- OpenID 连接 (OIDC) / 开放式授权 (Oauth)
- 安全断言标记语言 (SAML)
- Kerberos
- 远程验证拨号用户服务 (RADIUS) / 增强型终端访问控制器访问控制系统 (TACACS+)

领域 6：
安全评估与测试

6.1 设计和验证评估、测试和审计策略

- 内部
- 外部
- 第三方

6.2 进行安全控制测试

- 漏洞评估
- 渗透测试
- 日志审查
- 综合交易
- 代码审查和测试
- 误用案例测试
- 测试覆盖率分析
- 接口测试
- 漏洞攻击模拟
- 合规检查

6.3 收集安全过程数据（例如，技术和管理）

- 帐户管理
- 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) 和业务连续性 (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 执行或协助安全审计

- 内部
- 外部
- 第三方

领域 7：安全运营

7.1 理解并遵守调查

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

7.2 执行记录和监控活动

- 入侵侦测与防御
- 安全信息与事件管理 (SIEM)
- 连续监控
- 出口监控
- 日志管理
- 威胁情报（例如，威胁提要、威胁捕获）
- 用户和实体行为分析 (UEBA)

7.3 执行配置管理 (CM)（例如，预配、基线、自动化）

7.4 应用基本的安全操作概念

- 因需可知 / 最小权限
- 职责分离 (SoD) 和责任
- 特权账户管理
- 岗位轮换
- 服务等级协议 (SLA)

7.5 应用资源保护

- 媒介管理
- 媒体保护技术

7.6 执行事故管理

- 检测
- 响应
- 缓释
- 报告
- 恢复
- 补救
- 经验教训

7.7 执行和维护检测和预防措施

- 防火墙（例如，下一代、web 应用程序，网络）
- 入侵检测系统 (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
- 沙箱
- 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 实施和支持补丁和漏洞管理

7.9 理解并参与变更管理过程

7.10 执行恢复策略

- 备份存储策略
- 站点恢复策略
- 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 执行灾难恢复 (DR) 过程

- 响应
- 人员
- 通信
- 评估
- 修复
- 培训和意识
- 经验教训

7.12 测试灾难恢复计划 (DRP)

- 缓存回调/桌面
- 巡检
- 模拟
- 并行
- 全面中断

7.13 参与业务连续性 (BC) 计划的制定和演练

7.14 执行并管理物理安全

- 外围安全控制
- 内部安全控制

7.15 解决人员安全问题

- 出差
- 安全培训和意识
- 应急管理
- 胁迫

领域 8：
软件开发安全

8.1 理解安全并将其融入软件开发生命周期 (SDLC) 中

» 开发方法（例如，Agile、Waterfal、DevOps、DevSecOps)
» 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))
» 操作与维护
» 变更管理
» 综合产品团队 (IPT)

8.2 在软件开发环境中识别和应用安全控制

» 编程语言
» 库
» 成套工具
» 集成开发环境 (IDE)
» 运行时间
» 持续集成和持续交付 (CI/CD)
» 安全编排自动化与响应 (SOAR)
» 软件配置管理 (SCM)
» 代码存储库
» 应用程序安全性测试（例如，静态应用程序安全测试 (SAST)、动态应用程序安全测试 (DAST))

8.3 评估软件安全的有效性

» 更改审核和记录
» 风险分析和缓释

8.4 评估获得软件对安全的影响

» 商业成品 (COTS)
» 开源
» 第三方
» 托管服务（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准则和标准

» 源代码级安全弱点和漏洞
» 应用编程接口 (API) 安全
» 安全编码实践
» 软件定义安全

附加考试信息

补充参考

鼓励考生通过回顾有关 CBK 的相关资源，找出可能需要额外注意的研究领域来补充他们的教育知识和经验。

请访问网站 www.isc2.org/certifications/References 查看补充参考的完整列表。

考试政策和程序

(ISC)² 建议 CISSP 考生在报名参加考试前了解考试政策和程序。请访问网站 www.isc2.org/Register-for-Exam 阅读这项重要信息的详尽细目。

法律信息

有关 (ISC)² 法律政策的任何问题，请发送电子邮件至 legal@isc2.org 联系 (ISC)² 法务部。

有任何问题?

(ISC)² 参试服务部
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² 美洲区
电话：+1.866.331.ISC2 (4722)
电子邮件：info@isc2.org

(ISC)² 亚太地区
电话：+(852) 28506951
电子邮件：isc2asia@isc2.org

(ISC)² 欧洲、中东及非洲地区
电话：+44 (0)203 300 1625
电子邮件：info-emea@isc2.org