CISSP®

Certified Information Systems Security Professional

注册信息系统安全师

考试大纲

生效期：2018年4月

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

关于CISSP

注册信息系统安全师（CISSP）是全球最受广泛认可的信息安全认证。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的公共知识体系（CBK）中包含的广泛议题确保了与信息安全领域中所有原理的相关性。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
- 身份与访问管理
- 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(ISC)² 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，以及(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（Associate）。(ISC)²的准会员可以用接下来的6年时间积累所需工作经验。

认可

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

工作任务分析（Job Task Analysis）

(ISC)²对其会员有义务维护CISSP的关联性。定期进行工作任务分析（JTA）是一项系统而关键的过程，用来确定由CISSP安全专业人士所从事的工作。JTA的分析结果会用来更新考试。这个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）的考试信息

CISSP的所有英语考试都采用计算机自适应测试（CAT）。CISSP的其它语种的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道至150道
考题格式	多项选择和高级创新型考题
及格线	1000分中得到700分
可提供的考试语言	英语
测试中心	(ISC)² 授权的、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	14%
5.身份与访问管理 （IAM）	13%
6.安全评估与测试	12%
7.安全运营	13%
8.软件开发安全	10%
总计：	100%

CISSP线性考试信息

考试时长	6小时
考题数量	250道
考题格式	多项选择和高级创新型考题
及格线	1000分中得到700分
可提供的考试语言	法语、德语、巴西葡萄牙语、西班牙语、日语、简体中文、韩语
测试中心	(ISC)² 授权的、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	14%
5.身份与访问管理 （IAM）	13%
6.安全评估与测试	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 理解和运用保密性、完整性和可用性的概念

1.2 评估和应用安全治理的原理

» 将安全功能与商业策略、目标、使命和宗旨相连接
» 组织的流程 （例如购置、剥离、治理委员会）
» 组织的角色与职责
» 安全控制框架
» 谨慎考虑/恪尽职守

1.3 确定合规要求

» 合约、法律、行业标准和监管的要求
» 隐私的要求

1.4 理解与信息安全的全球背景相关的法律和监管问题

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

1.5 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

1.6 开发、撰写与实现安全政策、标准、流程和指南

1.7 对业务连续性（Business Continuity）进行识别、分析及优先级排序

» 制定并记录范围和计划
» 经营影响分析 （BIA）

1.8 促进与实行人员安全的策略与流程

- 员工筛选与雇佣
- 雇佣合约与政策
- 入职与离职程序
- 供应商、顾问与承包商的合约与控制
- 合规策略要求
- 隐私策略要求

1.9 理解与运用风险管理的概念

- 识别威胁与漏洞
- 风险评估/分析
- 风险响应
- 对策选择与实现
- 控制措施适用的类型（例如：预防措施、检测措施和纠正措施
- 安全控制评估 (SCA)
- 监控与测量
- 资产估价
- 汇报
- 持续提高
- 风险框架

1.10 理解与运用威胁建模的概念和方法论

- 威胁建模的方法论
- » 威胁建模的概念

1.11 将基于风险的管理概念运用到供应链

- 与硬件、软件和服务相关的风险
- » 第三方评估与监测
- » 最低安全需求
- 服务水平要求

1.12 建立与维护安全意识、教育和培训计划

- 安全意识宣贯与培训的方法和技术
- »定期内容审查
- »方案效果评价

领域 2: 资产安全

2.1 识别与分类信息和资产

» 数据分级
» 资产分级

2.2 确定与维护信息和资产所有权

2.3 保护隐私

» 数据所有者
» 数据所有者
» 数据残留
» 数据收集限制

2.4 确保适当的资产保留

2.5 确定数据安全控制

» 理解数据状态
» 定界与定制
» 标准选择
» 数据保护的方法

2.6 建立信息和资产的处理要求

领域 3:
安全架构与工程

3.1 使用安全设计原理来实施与管理工程的进程

3.2 理解安全模型的基本概念

3.3 基于系统安全需求选择控制措施

3.4 理解信息系统的安全功能（例如：内存保护、可信平台模块（TPM）、加密/解密）

3.5 评估与缓解安全架构、设计和解决方案要素的漏洞

- 基于客户端的系统
- 基于服务端的系统
- 数据库系统
- 密码系统
- 工业控制系统（ICS）
- 基于云端的系统
- 分布式系统
- 物联网（IoT）

3.6 评估和缓解Web系统中的漏洞

3.7 评估与缓解移动系统的漏洞

3.8 评估与缓解嵌入式设备的漏洞

3.9 运用密码学

- 密码生命周期 （例如：密钥管理、算法选择）
- 加密方法（例如：对称、非对称、椭圆曲线）
- 公钥基础设施 （PKI）
- 密钥管理实践
- 数字签名
- 抗抵赖性
- 完整性 （例如：哈希函数）
- 理解密码攻击方法
- 数字版权管理（DRM）

3.10 将安全原理运用到场所与设施的设计上

3.11 实施场所与设施的安全控制

» 配线柜/中继配线设施
» 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

领域 4:
通信与网络安全

4.1 在网络架构中实施安全设计原则

- 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（TCP/IP）网络
- 多层协议的作用
- 聚合协议
- 软件定义网络
- 无线网络

4.2 网络组件安全

- 硬件操作
- 传输介质
- 网络访问控制（NAC）设备
- 端点安全
- 内容配送网

4.3 根据设计实施安全通信通道

- 语音
- 多媒体协作
- 远程访问
- 数据通信
- 虚拟化网络

领域 5:
身份与访问管理 (IAM)

5.1 控制对资产的物理和逻辑访问

- 信息
- 系统
- 设备
- 设施

5.2 管理对人员、设备和服务的身份识别与验证

- 实施身份管理
- 单/多因素身份验证
- 可核查性
- 会话管理
- 身份注册与证明
- 联合身份管理 (FIM)
- 凭证管理系统

5.3 集成身份为第三方服务

- 内部部署
- 云计算
- 联合

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)

5.5 管理身份和访问配置生命周期

- 用户访问审查
- 系统账户访问审查
- 配置与清除配置

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 对安全控制进行测试

» 漏洞评估
» 渗透测试
» 日志审查
» 模拟交易
» 代码审查和测试
» 误用案例测试
» 测试覆盖率分析
» 接口测试

6.3 收集安全流程数据 (如：技术和管理)

» 账户管理
» 管理层审查和批准
» 关键业绩和风险指标
» 备份验证数据
» 信息安全意识宣贯
» 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

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 理解和支持调查

- 证据采集和处理
- 报告和记录
- 调查技术
- 数字取证工具、策略和程序

7.2 了解调查类型的要求

- 行政
- 刑事
- 民事
- 监管
- 行业标准

7.3 进行日志记录和持续监测活动

- 入侵检测和防御
- 安全信息和事件管理 (SIEM)
- 不间断持续监测
- 输出流量持续监测

7.4 安全配置资源

- 资产清单
- 资产管理
- 配置管理

7.5 理解和应用基本的安全运营概念

- 因需可知 / 最低权限
- 职责分离
- 特权帐户管理
- 岗位轮换
- 信息生命周期
- 服务水平协议（SLA）

7.6 应用资源保护技术

- 介质管理
- 硬件和软件资产管理

7.7 执行事件管理

- 检测
- 响应
- 缓解
- 报告
- 恢复
- 补救
- 经验教训

7.8 检测和预防措施的运营及维护

- 防火墙
- 入侵检测和防御系统
- 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

7.9 实施和支持补丁和漏洞管理

7.10 理解并参与变更管理流程

7.11 实施灾难恢复（DR）过程

- 备份存储策略
- 恢复站点策略
- 多个处理站点
- 系统弹性、高可用性、服务质量 (QoS) 和容错

7.12 实施灾难恢复 (DR) 流程

- 响应
- 人员
- 通信
- 评估
- 恢复
- 培训和信息安全意识宣贯

7.13 测试灾难恢复计划 (DRP)

- 书面测试/测试
- 穿行测试
- 模拟测试
- 并行测试
- 全面中断测试

7.14 参与业务连续性 (BC) 计划制定和演练

7.15 实施和管理物理安全

- 外围安全控制
- 内部安全控制

7.16 解决人员安全问题

- 旅行
- 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
» 成熟度模型
» 运营和维护
» 变更管理
» 集成产品团队

8.2 开发环境中识别和应用安全控制

» 软件环境的安全
» 配置管理作为安全编码的一个方面

8.3 评估软件安全的有效性

» 审核和变更记录
» 风险分析和缓解

8.4 评估获得软件对安全的影响

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
» 应用编程接口安全
» 安全编码实践

附加考试信息

补充参考

鼓励应试者通过回顾有关CBK的相关资源，并找出可能需要额外注意的研究领域来补充他们的教育和经验。

在 www.isc2.org/certifications/References 网站中查看补充参考的完整书单

考试政策和规程

(ISC)² 建议 CISSP 考生在报名参加考试前到 www.isc2.org/Register-for-Exam 阅读有关考试政策和规程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，请致信 legal@isc2.org 与 (ISC)² 法律部门联系。

其他问题?

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

(ISC)² 美洲区
Tel: +1.866.331.ISC2 (4722)
Email: info@isc2.org

(ISC)² 亚太区
Tel: +(852) 28506951
Email: isc2asia@isc2.org

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