CCSP®

Certified Cloud Security Professional

ISC2 Certification

认证考试大纲

生效日期：2022 年 8 月 1 日

ISC2™

关于 CCSP 认证

ISC2 开发了注册云安全专家 (CCSP) 认证，以确保云安全专业人员在云安全设计、实现、架构、运营、控制和遵守监管要求方面拥有所需的知识、技能和能力。CCSP认证将信息安全专业知识应用到云计算环境中，展示了云安全专业人员在云安全架构、设计、运营和服务编排方面的能力。这一专业能力根据全球公认的知识体系来衡量。

CCSP认证知识体系中包含的主题确保其与云安全领域
所有学科的相关性。考试合格的考生能够胜任以下六个领域的工作：

- 云概念、架构和设计
- 云数据安全
- 云平台和基础架构安全
- 云应用安全
- 云安全运营
- 法律、风险和合规

经验要求

考生必须在 IT 领域累计有至少五年全职工作经验。
其中三年必须在网络安全领域。此外，在《CCSP 考试大纲》六个领域中的一个或以上领域至少有一年的工作经验。如果您拥有计算机科学、IT或相关领域的学士学位或更高的学位，最多可减免一年的工作经验要求。拥有 ISC2 批准的清单中的其他认证证书，可以减免 CCSP 考试大纲六大领域中一个或一个以上领域的一年工作经验要求。持有有效的 CISSP 证书，可减免全部 CCSP 工作经验要求。兼职工作和实习也可计入作经验要求。

不具备 CCSP 所需经验的考生，可以通过 CCSP 考试成为 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。有关 CCSP 经验要求以及如何计算兼职工作和实习经验的更多信息，请访问 www.isc2.org/Certifications/CCSP/experience-requirements。

认证

CCSP 认证符合 ANSI/ISO/IEC 17024 标准的严格要求。

工作任务分析 (JTA)

ISC2 有义务为其成员保持 CCSP 的相关性。定期进行的“工作任务分析”（JTA）是一项有序而关键的过程，旨在确定从事 CCSP 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。此过程确保考生的测试题目与目前从业的专注于云技术的信息安全专业人士的角色和职责密切相关。

CCSP 考试信息

考试时长	4 小时
题目数量	150
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、德语和日语
考试中心	Pearson VUE 考试中心

自 2024 年 8 月 1 日起，CCSP 考试包括 125 道选择题，时长 3 小时。

CCSP 考试的权重

领域	权重
1.云概念、架构和设计	17%
2. 云数据安全	20%
3. 云平台和基础架构安全	17%
4. 云应用安全	17%
5. 云安全运营	16%
6. 法律、风险和合规	13%
总计：	**100%**

领域 1：
云概念、架构和设计

1.1 了解云计算概念

» 云计算定义
» 云计算角色和职责（例如，云服务客户、云服务提供商、云服务合作伙伴、云服务代理、监管机构）
» 云计算关键特性（例如，按需自助服务、广泛的网络访问、多租户、快速弹性和可伸缩性、资源池化、可度量服务）
» 构建块技术（例如，虚拟化、存储、联网、数据库、编排）

1.2 描述云计算参考架构

» 云计算活动
» 云服务能力（如应用能力类型、平台能力类型、基础架构能力类型）
» 云服务类别（例如，软件即服务 (SaaS)、基础架构即服务 (IaaS)、平台即服务 (PaaS)）
» 云部署模型（例如，公共云、私有云、混合云、社区云、多云）
» 云共享考虑因素（例如，互操作性、可移植性、可逆性、可用性、安全性、隐私、弹性、性能、治理、维护和版本控制、服务等级和服务等级协议 (SLA)、可审计性、监管、外包）
» 相关技术的影响（例如，数据科学、机器学习、人工智能 (AI)、区块链、物联网 (IoT)、容器、量子计算、边缘计算、机密计算、DevSecOps）

1.3 了解与云计算相关的安全概念

» 密码学和密钥管理
» 身份和访问控制（例如，用户访问、特权访问、服务访问）
» 数据和媒介清理（例如，覆盖、加密擦除）
» 网络安全（例如，网络安全组、流量检查、地理围栏、零信任网络）
» 虚拟化安全（例如，hypervisor 安全、容器安全、临时计算、无服务器技术）
» 常见威胁
» 安全卫生（例如，打补丁、基线）

1.4 了解安全云计算的设计原则

» 云安全数据生命周期
» 基于云的业务持续性 (BC) 和灾难恢复 (DR) 计划
» 业务影响分析 (BIA)（例如，成本效益分析、投资回报率 (ROI)）
» 功能安全需求（例如，可移植性、互操作性、供应商锁定）
» 不同云类别的安全注意事项和责任（例如，软件即服务 (SaaS)、基础架构即服务 (IaaS)、平台即服务 (PaaS)）
» 云设计模式（例如，SANS 安全原则、架构完善的框架、云安全联盟 (CSA) 企业架构）
» DevOps 安全

1.5 评估云服务提供商

» 根据标准进行验证（例如，国际标准组织/国际电子技术委员会 (ISO/IEC) 27017、支付卡行业数据安全标准 (PCI DSS)）
» 系统/子系统产品认证（例如，通用标准 (CC)、联邦信息处理标准 (FIPS) 140-2）

领域 2：云数据安全

2.1 描述云数据概念

» 云数据生命周期阶段
» 数据分散
» 数据流

2.2 设计和实现云数据存储架构

» 存储类型（例如，长期、临时、原始存储）
» 对存储类型的威胁

2.3 设计和应用数据安全技术和策略

» 加密和密钥管理
» 散列
» 数据混淆（例如，屏蔽、匿名化）
» 令牌化
» 数据丢失防护 (DLP)
» 密钥、机密和证书管理

2.4 实现数据发现

» 结构化数据
» 非结构化数据
» 半结构化数据
» 数据位置

2.5 计划和实现数据分类

» 数据分类策略
» 数据映射
» 数据标签

2.6 设计和实现信息权限管理 (IRM)

» 目标（例如，数据权限、服务预置(provisioning)、访问模型）
» 适当的工具（例如，颁发和撤销证书）

2.7 规划和实施数据保留、删除和归档策略

» 数据保留策略
» 数据删除程序和机制
» 数据归档程序和机制
» 依法保留

2.8 设计并实现数据事件的可审计性、可追溯性和可问责性

» 事件源的定义和事件属性的要求（例如，身份、互联网协议 (IP) 地址、地理位置）
» 数据事件的日志记录、存储和分析
» 监管链和不可抵赖性

领域 3：云平台和基础架构 安全

3.1 理解云基础架构和平台组件

- 物理环境
- 网络与通信
- 计算
- 虚拟化
- 存储
- 管理平面

3.2 设计安全的数据中心

- 逻辑设计（例如，租户分区、访问控制）
- 物理设计（例如，位置、购买或建造）
- 环境设计（例如，供暖、通风与空调 (HVAC)、多供应商通路连接）
- 设计弹性

3.3 分析与云基础架构和平台相关的风险

- 风险评估（例如，识别、分析）
- 云漏洞、威胁和攻击
- 风险缓解策略

3.4 计划和实现安全控制

- 物理和环境保护（例如，内部部署）
- 系统、存储和通信保护
- 云环境中的识别、认证和授权
- 审计机制（例如，日志收集、关联、数据包捕获）

3.5 计划业务持续性 (BC) 和灾难恢复 (DR)

- 业务持续性 (BC) / 灾难恢复 (DR) 策略
- 业务需求（例如，恢复时间目标 (RTO)、恢复点目标 (RPO)、恢复服务级别）
- 计划的创建、实施和测试

领域 4：云应用安全

4.1 倡导应用程序安全性的培训和意识

» 云开发基础
» 常见陷阱
» 常见云漏洞（例如，开放网端应用安全项目 (OWASP) 10 大风险、SANS 前 25 个最危险的软件错误）

4.2 描述安全软件开发生命周期 (SDLC) 流程

» 业务需求
» 阶段和方法（例如，设计、编码、测试、维护、瀑布式与敏捷式）

4.3 应用安全软件开发生命周期 (SDLC)

» 云特定风险
» 威胁建模（例如，哄骗、篡改、抵赖、信息泄露、拒绝服务和特权提升 (STRIDE)；灾难、可重现性、可利用性、受影响用户与可发现性 (DREAD)；架构、威胁、攻击面和缓解措施 (ATASM)；攻击模拟和威胁分析过程 (PASTA)）
» 避免开发过程中的常见漏洞
» 安全编码（例如，开放网端应用安全项目 (OWASP) 应用安全检验标准 (ASVS)、卓越代码软件保障论坛 (SAFECode)）
» 软件配置管理和版本控制

4.4 应用云软件保障和验证

» 功能和非功能测试
» 安全测试方法（例如，黑盒、白盒、静态、动态、软件组成分析 (SCA)、交互式应用程序安全测试 (IAST)）
» 质量保证 (QA)
» 滥用案例测试

4.5 使用经过验证的安全软件

» 保护应用编程接口 (API)
» 供应链管理（例如，供应商评估）
» 第三方软件管理（例如，许可）
» 经过验证的开源软件

4.6 了解云应用架构的细节

» 补充安全组件（例如，网端应用防火墙 (WAF)、数据库活动监控 (DAM)、可扩展标记语言 (XML) 防火墙、应用编程接口 (API) 网关）
» 密码学
» 沙盒化
» 应用程序虚拟化和编排（例如，微服务、容器）

4.7 设计适当的身份和访问管理 (IAM) 解决方案

» 联合身份
» 身份提供商 (IdP)
» 单点登录 (SSO)
» 多因子验证 (MFA)
» 云访问安全代理 (CASB)
» 机密管理

领域 5：云安全运营

5.1 为云环境构建以及实现物理和逻辑基础架构

» 硬件特定的安全配置要求（例如，硬件安全模块 (HSM) 和可信赖平台模块 (TPM)）
» 管理工具的安装和配置
» 虚拟硬件特定的安全配置要求（例如，网络、存储、内存、中央处理器 (CPU)、Hypervisor 类型 1 和 2）
» 安装客户机操作系统 (OS) 虚拟化工具集

5.2 运行和维护云环境的物理和逻辑基础架构

» 本地和远程访问的访问控制（例如，远程桌面协议 (RDP)、安全终端访问、安全外壳 (SSH)、基于控制台的访问机制、跳板机、虚拟客户端）
» 安全网络配置（例如，虚拟局域网 (VLAN)、传输层安全 (TLS)、动态主机配置协议 (DHCP)、域名系统安全扩展 (DNSSEC)、虚拟专用网络 (VPN)）
» 网络安全控制（例如防火墙、入侵检测系统 (IDS)、入侵防御系统 (IPS)、蜜罐、漏洞评估、网络安全组、堡垒主机）
» 通过应用基线、监控和修复来强化操作系统 (OS)（例如 Windows、Linux、VMware）
» 补丁管理
» 基础架构即代码 (IaC) 策略
» 集群主机的可用性（如分布式资源调度、动态优化、存储集群、维护模式、高可用性（HA））
» 客户机操作系统 (OS) 的可用性
» 性能和容量监控（例如，网络、计算、存储、响应时间）
» 硬件监控（例如，磁盘、中央处理器 (CPU)、风扇速度、温度）
» 主机和客户机操作系统 (OS) 备份和恢复功能的配置
» 管理平面（例如，调度、编排、维护）

5.3 实施运营控制和标准（例如，信息技术基础架构库 (ITIL)、国际标准组织/国际电子技术委员会 (ISO/IEC) 20000-1）

- 变更管理
- 持续性管理
- 信息安全管理
- 持续的服务改进管理
- 事故管理
- 问题管理
- 发布管理
- 部署管理
- 配置管理
- 服务等级管理
- 可用性管理
- 容量管理

5.4 支持数字取证

- 取证数据收集方法
- 证据管理
- 收集、获取和保存数字证据

5.5 管理与相关方的沟通

- 供应商
- 客户
- 合作伙伴
- 监管机构
- 其他利益相关者

5.6 管理安全运营

- 安全运营中心 (SOC)
- 安全控制的智能监控（例如，防火墙、入侵检测系统 (IDS)、入侵防御系统 (IPS)、蜜罐、网络安全组、人工智能 (AI)）
- 日志捕获和分析（例如，安全信息和事件管理 (SIEM)、日志管理）
- 事故管理
- 漏洞评估

领域 6：法律、风险和合规

6.1 明确云环境中的法律要求和独特风险

» 国际法律冲突
» 云计算特有的法律风险评估
» 法律框架和准则
» 电子取证（eDiscovery）（例如，国际标准组织/国际电子技术委员会（ISO/IEC）27050、云安全联盟（CSA）指南）
» 取证要求

6.2 了解隐私问题

» 合同规定的和受监管的私人数据之间的区别（例如，受保护的健康信息（PHI）、个人可识别信息（PII））
» 与私人数据相关的国家特定立法（例如，受保护的健康信息（PHI）、个人可识别信息（PII））
» 数据隐私的司法管辖区差异
» 标准隐私要求（例如，国际标准组织/国际电子技术委员会（ISO/IEC）27018、普遍接受的隐私原则（GAPP）、一般数据保护条例（GDPR））
» 隐私影响评估（PIA）

6.3 了解云环境的审计流程、方法和必要的调整

» 内部和外部审计控制
» 审计要求的影响
» 确定虚拟化和云的保障挑战
» 审计报告的类型（例如，关于认证业务标准的声明（SSAE）、服务组织控制（SOC）、国际鉴证业务准则（ISAE））
» 审计范围声明的限制（例如，关于认证业务标准的声明（SSAE）、国际鉴证业务准则（ISAE））
» 差距分析（例如，控制分析、基线）
» 审计计划
» 内部信息安全管理系统
» 内部信息安全控制系统
» 政策（例如，组织、功能、云计算）
» 相关利益相关者的识别和参与
» 受到严格监管行业的特殊合规要求（例如，北美电力可靠性公司/关键基础设施保护（NERC / CIP）、健康保险便捷与责任法案（HIPAA）、经济与临床医疗保健信息科技（HITECH）法案、支付卡行业（PCI））
» 分布式信息技术（IT）模型的影响（例如，不同的地理位置和跨越法律管辖区）

6.4 了解云对企业风险管理的影响

» 评估提供商的风险管理计划（如控制、方法、政策、风险状况、风险偏好等）
» 数据所有者/控制者与数据保管者/处理者之间的区别
» 监管透明度要求（例如，违规通知、Sarbanes-Oxley (SOX)、一般数据保护条例 (GDPR)）
» 风险处理（即规避、减轻、转移、共享、接受）
» 不同的风险框架
» 风险管理指标
» 风险环境评估（例如，服务、供应商、基础架构、业务）

6.5 了解外包和云合同设计

» 业务要求（例如，服务等级协议 (SLA)、主服务协议 (MSA)、工作陈述 (SOW)）
» 供应商管理（例如，供应商评估、供应商锁定风险、供应商生存能力、托管）
» 合同管理（例如，审计权、指标、定义、终止、诉讼、保证、合规、访问云/数据、网络风险保险）
» 供应链管理（例如国际标准组织/国际电子技术委员会 (ISO/IEC) 27036）

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。

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

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解。

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) 58035662
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