CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

자격증 시험 개요

발효일: 2022년 8월 1일

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

CCSP 소개

(ISC)²는 클라우드 보안 전문가가 클라우드 보안 설계, 구현, 아키텍처, 운영, 제어 및 규정 프레임워크 준수에 필요한 지식, 기술 및 능력을 갖추도록 하기 위해 공인 클라우드 보안 전문가(CCSP) 자격 증명을 개발했습니다. CCSP는 정보 보안 전문 지식을 클라우드 컴퓨팅 환경에 적용하고 클라우드 보안 아키텍처, 설계, 운영 및 서비스 오케스트레이션에 대한 역량을 나타냅니다. 이러한 전문적인 역량은 전세계적으로 인정된 지식 체계를 기준으로 측정됩니다.

CCSP 지식의 공통체(CBK)에 포함된 주제는 클라우드 보안 분야의 모든 영역에서 관련성을 보장합니다. 합격자는 다음 6개 분야에 관한 능력을 입증합니다.

- 클라우드 개념, 아키텍처 및 설계
- 클라우드 데이터 보안
- 클라우드 플랫폼 및 인프라 보안
- 클라우드 어플리케이션 보안
- 클라우드 보안 관제
- 법률, 위험 및 규정 준수

경력 요구 사항

응시자는 정보 기술 분야에서 최소 5년의 누적 유급 업무 경험이 있어야 하며, 그 중 3년은 정보 보안 분야에서, 1년은 CCSP CBK의 6개 영역 중 하나 이상에서 근무해야 합니다. CSA의 CCSK 인증서를 취득하면 CCSP CBK의 6개 영역 중 하나 이상에서 1년 간의 경험을 대체할 수 있습니다. (ISC)²의 CISSP 자격증 획득은 전체 CCSP 경력 요구사항을 대체할 수 있습니다.

CCSP가 되는데 필요한 경력이 없는 응시자는 CCSP 시험을 성공적으로 통과하여 Associate of (ISC)² 이 될 수 있습니다. Associate of (ISC)² 은 5년의 필수 경력을 쌓기 위해 6년의 기간이 주어집니다. CSSP 경력 요건과 파트 타임 근로 및 인턴십을 환산하는 방법에 대한 자세한 사항은 www.isc2.org/Certifications/CSSP/experience-requirements에서 확인하십시오.

인증

CCSP는 ANSI/ISO/IEC 표준 17024의 엄격한 요구 사항을 준수합니다.

직무 과제 분석(JTA)

(ISC)²는 회원들을 위해 CSSP의 적합성 유지의 의무를 갖습니다. 정기적으로 수행되는 직무 과제 분석(JTA)은 CSSP에서 정의한 직업에 종사하는 보안 전문가가 수행하는 과제를 결정하는 체계적이고 중요한 프로세스입니다. JTA의 결과는 시험을 업데이트하는 데 사용됩니다. 이 과정을 통해 응시자는 클라우드 기술에 집중하는 오늘날의 현업 종사 정보 보안 전문가의 역할 및 책임과 관련된 주제 분야에서 테스트를 거치게 됩니다.

CSSP 시험 정보

시험 시간	4시간
문항 수	150
문제 형식	선다형 문제
합격 기준	700점 이상(총점 1000점)
시험 가능 여부	영어, 한국어, 중국어, 일본어, 독일어, 스페인어
테스트 센터	Pearson VUE 테스트 센터

CSSP 시험 가중치

분야	가중치
1. 클라우드 개념, 아키텍처 및 설계	17%
2. 클라우드 데이터 보안	20%
3. 클라우드 플랫폼 및 인프라 보안	17%
4. 클라우드 어플리케이션 보안	17%
5. 클라우드 보안 관제	16%
6. 법률, 위험 및 규정 준수	13%
총:	100%

분야 1:
클라우드 개념, 아키텍처 및 설계

1.1 클라우드 컴퓨팅 개념 이해

- 클라우드 컴퓨팅 정의
- 클라우드 컴퓨팅 역할 및 책임(예: 클라우드 서비스 고객, 클라우드 서비스 제공자, 클라우드 서비스 파트너, 클라우드 서비스 브로커, 규제 기관)
- 주요 클라우드 컴퓨팅 특성(예: 주문형 셀프 서비스, 광범위한 네트워크 액세스, 멀티 테넌시, 빠른 탄력성 및 확장성, 리소스 풀링, 측정되는 서비스)
- 빌딩 블록 기술(예: 가상화, 스토리지, 네트워킹, 데이터베이스, 오케스트레이션)

1.2 클라우드 참조 아키텍처 묘사

- 클라우드 컴퓨팅 활동
- 클라우드 서비스 기능(예: 어플리케이션 기능 유형, 플랫폼 기능 유형, 인프라 기능 유형)
- 클라우드 서비스 카테고리(예: 소프트웨어형 서비스(SaaS), 서비스 형태 인프라(IaaS), 플랫폼형 서비스(PaaS))
- 클라우드 배포 모델(예: 공용, 사설, 하이브리드, 커뮤니티, 멀티 클라우드)
- 클라우드 공유 고려 사항(예: 상호 운용성, 이식성, 가역성, 가용성, 보안, 개인 정보 보호, 복원력, 성능, 거버넌스, 유지 관리 및 버전 관리, 서비스 수준 및 서비스 수준 협약(SLA), 감사 가능성, 규제, 아웃소싱)
- 관련 기술의 영향(예: 데이터 과학, 머신 러닝, 인공지능(AI), 블록체인, 사물 인터넷(IoT), 컨테이너, 퀀텀 컴퓨팅, 에지 컴퓨팅, 기밀 컴퓨팅, DevSecOps)

1.3 클라우드 컴퓨팅과 관련된 보안 개념 이해

- 암호화 및 키 관리
- ID 및 액세스 제어(예: 사용자 액세스, 권한 액세스, 서비스 액세스)
- 데이터 및 미디어 위생 처리(예: 덮어쓰기, 암호화 지우기)
- 네트워크 보안(예: 네트워크 보안 그룹, 트래픽 검사, 지오펜싱, 제로 트러스트 네트워크)
- 가상화 보안(예: 하이퍼바이저 보안, 컨테이너 보안, 임시 컴퓨팅, 서버리스 기술)
- 공통 위협
- 보안 위생(예: 패치 적용, 기준 설정)

1.4 보안 클라우드 컴퓨팅의 설계 원칙 이해

- 클라우드 보안 데이터 수명주기
- 클라우드 기반 사업 연속성 (BC) 및 재난 복구 (DR) 계획
- 사업 영향 분석(BIA)(예: 비용-편익 분석, 투자 수익(ROI))
- 기능적 보안 요구 사항(예: 이식성, 상호 운용성, 벤더 종속성)
- 다양한 클라우드 범주에 대한 보안 고려 사항 및 책임(예: 소프트웨어형 서비스(SaaS), 서비스 형태 인프라(IaaS), 플랫폼형 서비스(PaaS))
- 클라우드 설계 패턴(예: SANS 보안 원칙, 잘 설계된 프레임워크, Clould Security Alliance (CSA) 엔터프라이즈 아키텍처)
- DevOps 보안

1.5 클라우드 서비스 제공자 평가

- 기준에 대한 검증(예: 국제 표준화 기구/국제 전기 기술 위원회(ISO/IEC) 27017, 결제 카드 산업 정보보안 표준(PCI DSS))
- 시스템/하위 시스템 제품 인증(예: 공통 기준(CC), 연방 정보 처리 표준(FIPS) 140-2)

분야 2:
클라우드 데이터 보안

2.1 클라우드 데이터 개념 묘사

- 클라우드 데이터 수명주기 단계
- 데이터 분산
- 데이터 흐름

2.2 클라우드 데이터 스토리지 아키텍처 설계 및 구현

- 스토리지 유형(예: 장기, 임시, 로우 스토리지)
- 스토리지 유형에 대한 위협

2.3 데이터 보안 기술 및 전략 설계 및 적용

- 암호화 및 키 관리
- 해싱
- 데이터 난독화(예: 마스킹, 익명화)
- 토큰화
- 데이터 손실 방지(DLP)
- 키, 비밀 및 인증서 관리

2.4 데이터 검색 구현

- 구조화된 데이터
- 비구조화된 데이터
- 반구조화된 데이터
- 데이터 위치

2.5 데이터 분류 계획 및 구현

- 데이터 분류 정책
- 데이터 매핑
- 데이터 라벨링

2.6 정보 권리 관리(IRM) 설계 및 구현

- 목표(예: 데이터 권한, 프로비저닝, 액세스 모델)
- 적절한 도구(예: 인증서 발급 및 취소)

2.7 데이터 보존, 삭제 및 보관 정책 계획 및 구현

- 데이터 유지 정책
- 데이터 삭제 절차 및 메커니즘
- 데이터 보관 절차 및 메커니즘
- 증거보존 통지

2.8 데이터 이벤트의 감사성, 추적성 및 책임성을 설계 및 구현

- 이벤트 소스 정의 및 이벤트 속성 요구 사항(예: ID, 인터넷 프로토콜(IP) 주소, 지리적 위치)
- 데이터 이벤트의 로깅, 저장 및 분석
- 관리 연속성 및 부인 방지

분야 3: 클라우드 플랫폼 및 인프라 보안

3.1 클라우드 인프라 및 플랫폼 구성 요소 이해

- 물리적 환경
- 네트워크 및 통신
- 컴퓨팅
- 가상화
- 스토리지
- 관리 플레인

3.2 안전한 데이터 센터 설계

- 논리적 설계(예: 테넌트 분할, 액세스 제어)
- 물리적 디자인(예: 위치, 구매 또는 구축)
- 환경 설계(예: 난방, 통풍 및 공조(HVAC), 다중 벤더 경로 연결)
- 설계 탄력성

3.3 클라우드 인프라 및 플랫폼과 관련된 위험 분석

- 위험 평가(예: 식별, 분석)
- 클라우드 취약점, 위협 및 공격
- 위험 완화 전략

3.4 보안 통제 계획 및 구현

- 물리적 및 환경적 보호(예: 온프레미스)
- 시스템, 스토리지 및 통신 보호
- 클라우드 환경에서 식별, 인증 및 권한 부여
- 감사 메커니즘(예: 로그 수집, 상관 관계, 패킷 캡처)

3.5 사업 연속성(BC) 및 재난 복구(DR) 계획

- 사업 연속성(BC)/재난 복구(DR) 전략
- 비즈니스 요구 사항(예: 목표 복구 시간(RTO), 목표 복구 지점(RPO), 복구 서비스 수준)
- 계획 생성, 구현 및 테스트

분야 4:
클라우드 어플리케이션 보안

4.1 어플리케이션 보안에 대한 교육 및 인식 옹호

- 클라우드 개발 기본
- 공통 함정
- 공통 클라우드 취약점(예: Open Web Application Security Project (OWASP) 탑 10, SANS 탑 25)

4.2 소프트웨어 개발 생애주기(SDLC) 프로세스 설명

- 비즈니스 요구 사항
- 단계 및 방법론(예: 설계, 코드, 테스트, 유지 관리, 워터폴 대 애자일)

4.3 소프트웨어 개발 생애주기(SDLC) 적용

- 클라우드 관련 위험
- 위협 모델링(예: 스푸핑, 변조, 부당 변경, 거부, 정보 유출, 서비스 거부, 권한 상승(STRIDE), 위험, 재현확률, 공격 용이도, 영향 받는 사용자, 발견 이도 (DREAD), 아키텍처, 위협, 공격 표면 및 완화(ATASM), 공격 모의실험 및 위협 분석 과정 (PASTA))
- 개발 중 일반적인 취약점 방지
- 보안 코딩(예: Open Web Application Security Project (OWASP) 어플리케이션 보안 검증 표준 (ASVS), 코드의 우수성을 위한 소프트웨어 보증 포럼(SAFECode))
- 소프트웨어 구성 관리 및 버전 관리

4.4 클라우드 소프트웨어 보증 및 검증 적용

- 기능 및 비기능 테스트
- 보안 테스트 방법론(예: 블랙박스, 화이트박스, 정적, 동적, 소프트웨어 구성 분석(SCA), 어플리케이션 간 보안 테스트(IAST))
- 품질 보증(QA)
- 남용 사례 테스트

4.5 검증된 보안 소프트웨어 사용

- 어플리케이션 프로그램 인터페이스(APIs) 보안
- 공급망 관리(예: 벤더 평가)
- 제삼자 소프트웨어 관리(예: 라이선스)
- 검증된 오픈 소스 소프트웨어

4.6 클라우드 어플리케이션 아키텍처의 세부 사항 이해

- 추가 보안 구성요소(예: 웹 어플리케이션 방화벽(WAF), 데이터베이스 활동 감시(DAM), 확장형 생성 언어(XML) 방화벽, 어플리케이션 프로그램 인터페이스(API) 게이트웨이)
- 암호학
- 샌드박스
- 어플리케이션 가상화 및 오케스트레이션(예: 마이크로서비스, 컨테이너)

4.7 적절한 ID 및 접근 통제(IAM) 솔루션 설계

- 연합 ID
- ID 제공자(IdP)
- 통합 인증(SSO)
- 다중 인증(MFA)
- 클라우드 접근 보안 브로커(CASB)
- 비밀 관리

분야 5:
클라우드 보안 관제

5.1 클라우드 환경을 위한 물리적, 논리적 인프라 구축 및 구현

- 하드웨어별 보안 구성 요구 사항(예: 하드웨어 보안 모듈(HSM) 및 신뢰 기반체계 부품(TPM))
- 관리 도구의 설치 및 구성
- 가상 하드웨어별 보안 구성 요구 사항(예: 네트워크, 스토리지, 메모리, 중앙 처리 장치(CPU), 하이퍼바이저 유형 1 및 2)
- 게스트 운영 체제(OS) 가상화 도구 세트 설치

5.2 클라우드 환경을 위한 물리적, 논리적 인프라 운영 및 유지

- 로컬 및 원격 액세스를 위한 액세스 제어(예: 원격 데스크톱 프로토콜(RDP), 보안 터미널 액세스, 보안 쉘(SSH), 콘솔 기반 액세스 메커니즘, 점프박스, 가상 클라이언트)
- 보안 네트워크 구성(예: 가상 근거리 네트워크(VLAN), 전송 계층 보안(TLS), 동적 호스트 구성 프로토콜(DHCP), 도메인 네임 시스템 보안 확장기능(DNSSEC), 가상 사설망(VPN))
- 네트워크 보안 제어(예: 방화벽,침입 탐지 시스템(IDS), 침입 예방 시스템(IPS), 허니팟, 취약점 평가, 네트워크 보안 그룹, 배스천 호스트)
- 기준선, 모니터링 및 교정 적용을 통한 운영 체제(OS) 강화(예: Windows, Linux, VMware)
- 패치 관리
- 코드로 인프라 관리하기(IaC) 전략
- 클러스터된 호스트의 가용성(예: 분산 리소스 스케줄링, 동적 최적화, 스토리지 클러스터, 유지 관리 모드, 고가용성(HA))
- 게스트 운영 체제(OS) 가용성
- 성능 및 용량 모니터링(예: 네트워크, 컴퓨팅, 스토리지, 응답 시간)
- 하드웨어 모니터링(예: 디스크, 중앙 처리 장치(CPU), 팬 속도, 온도)
- 호스트 및 게스트 운영 체제(OS) 백업 및 복원 기능 구성
- 관리 평면(예: 스케줄링, 오케스트레이션, 유지 관리)

5.3 운영 제어 및 표준 구현(예: 정보 기술 인프라 라이브러리(ITIL), 국제 표준화 기구/국제 전자기술 위원회(ISO/IEC) 20000-1)

- 변경 관리
- 지속성 관리
- 정보 보안 관리
- 지속적인 서비스 개선 관리
- 사고 관리
- 문제 관리
- 릴리스 관리
- 배포 관리
- 구성 관리
- 서비스 수준 관리
- 가용성 관리
- 용량 관리

5.4 디지털 포렌식 지원

- 포렌식 데이터 수집 방법론
- 증거 관리
- 디지털 증거 수집, 획득 및 보존

5.5 관련 당사자와의 커뮤니케이션 관리

- 벤더
- 고객
- 파트너
- 규제 기관
- 기타 이해 관계자

5.6 클라우드 보안 관제

- 보안 관제 센터(SOC)
- 보안 제어의 지능형 모니터링(예: 방화벽, 침입 탐지 시스템(IDS), 침입 예방 시스템(IPS), 허니팟, 네트워크 보안 그룹, 인공 지능(AI))
- 로그 캡처 및 분석(예: 보안 정보 및 신호 관리(SIEM), 로그 관리)
- 사고 관리
- 취약점 평가

분야 6:
법률, 위험 및 규정 준수

6.1 클라우드 환경 내에서 법적 요구 사항과 고유한 위험을 명확히 표현

- 상충되는 국제법
- 클라우드 컴퓨팅 관련 법적 위험 평가
- 법적 프레임워크 및 지침
- eDiscovery(예: 국제 표준화 기구/국제 전기 기술 위원회(ISO/IEC) 27050, Cloud Security Alliance (CSA) 지침)
- 포렌식 요구사항

6.2 개인 정보 문제 이해

- 계약에 따른 개인 데이터와 규제 대상 개인 데이터의 차이점(예: 민감성 건강 정보(PHI), 개인 식별 정보(PII))
- 개인 데이터와 관련된 국가별 법률(예: 민감성 건강 정보(PHI), 개인 식별 정보(PII))
- 데이터 프라이버시의 관할권 차이
- 표준 개인 정보 보호 요구 사항(예: 국제 표준화 기구/국제 전기 기술 위원회(ISO/IEC) 27018, 일반적으로 허용되는 개인 정보 보호 원칙(GAPP), 일반 데이터 보호 규정(GDPR))
- 개인정보 영향 평가(PIA)

6.3 클라우드 환경에 대한 감사 프로세스, 방법론 및 필요한 적응 이해

- 내부 및 외부 감사 통제
- 감사 요구 사항의 영향
- 가상화 및 클라우드의 보증 문제 식별
- 감사 보고서 유형(예: 증명 업무 표준에 대한 명(SSAE), 서비스 조직 통제(SOC), 보증 업무에 관한 국제 표준(ISAE))
- 감사 범위 설명의 제한 사항(예: 증명 업무 준에 대한 성명(SSAE), 보증 업무에 관한 국제 표준(ISAE))
- 갭 분석(예: 통제 분석, 기준선)
- 감사 계획
- 내부 정보 보안 관리 시스템
- 내부 정보 보안 통제 시스템
- 정책(예: 조직적, 기능적, 클라우드 컴퓨팅)
- 관련 이해 관계자 식별 및 참여
- 규제가 엄격한 산업을 위한 전문적인 규정 준수 요구 사항(예: 북미 전기 신뢰성 공사/중요 기반 시설 보호(NERC/CIP), 건강보험 정보의 이전 및 그 책임에 관한 법률(HIPAA), 경제 및 임상 건강을 위한 건강 정보 기술(HITECH) 법, 결제 카드 산업(PCI))
- 분산된 정보 기술(IT) 모델의 영향(예: 다양한 지리적 위치 및 법적 관할 구역의 교차)

6.4 클라우드가 엔터프라이즈 위험 관리에 미치는 영향 이해

- 제공자 위험 관리 프로그램 평가(예: 통제, 방법론, 정책, 위험 프로필, 위험 선호도)
- 데이터 소유자/컨트롤러 vs. 데이터 관리자/프로세서의 차이점
- 규제 투명성 요구 사항(예: 위반 알림, 사베인 옥슬리(SOX), 일반 데이터 보호 규정(GDPR))
- 위험 처리(예: 회피, 완화, 이전, 공유, 수용)
- 다양한 위험 프레임워크
- 위험 관리를 위한 메트릭
- 위험 환경 평가(예: 서비스, 벤더, 인프라, 비즈니스)

6.5 아웃소싱 및 클라우드 계약 설계 이해

- 비즈니스 요구 사항(예: 서비스 수준 협약(SLA), 마스터 서비스 계약(MSA), 업무 기술서(SOW))
- 벤더 관리(예: 벤더 평가, 벤더 종속 위험, 벤더 성공 가능성, 에스크로)
- 계약 관리(예: 감사 권리, 메트릭, 정의, 종료, 소송, 보증, 규정 준수, 클라우드/데이터 액세스, 사이버 위험 보험)
- 공급망 관리(예: 국제 표준화 기구/국제 전기 기술 위원회(ISO/IEC) 27036)

시험 관련 추가 정보

추가 참조 사항

응시자는 CBK와 관련된 관련 자료를 검토하고 추가 관심이 필요한 부분을 확인함으로써 교육 및 경험을 보완할 것을 권장합니다.

추가 참조 전체 목록은 www.isc2.org/certifications/References에서 확인하십시오.

시험 정책 및 절차

(ISC)²는 CSSP 지원자가 시험에 등록하기에 앞서 시험 정책 및 절차를 검토할 것을 권장합니다. 다음의 중요한 정보에 대한 종합적인 내용은 www.isc2.org/Register-for-Exam 에서 확인하십시오.

법률 정보

(ISC)²의 법률 정책과 관련된 질문은 legal@isc2.org (ISC)²법무팀에 문의하십시오.

문의사항 연락처

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
전화번호: +1.727.785.0189
이메일: info@isc2.org

(ISC)² Asia-Pacific
전화번호: +852.5803.5662
이메일: isc2asia@isc2.org

(ISC)² EMEA
전화번호: +44 (0)203-960-7800
이메일: info-emea@isc2.org