CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

자격증 시험 개요

시행일: 2021년 5월 1일

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

CISSP 소개

공인 정보 시스템 보안 전문가(CISSP)는 정보 보안 업계에서 국제적으로 가장 널리 인정되는 자격증입니다. CISSP는 조직의 전반적인 보안 상태를 효과적으로 설계, 구축 및 관리하기 위해 요구되는 정보 보안 전문가의 심도 있는 기술 및 관리 지식과 경험을 검증합니다.

CISSP 정보 보안 지식 체계(CBK®)에 포함된 광범위한 주제는 정보 보안의 모든 분야와의 관련성을 보장합니다. 합격자는 다음 8개 분야에 관한 능력이 입증되는 것입니다:

- 보안 및 위험 관리
- 자산 보안
- 보안 아키텍처 및 엔지니어링
- 통신 및 네트워크 보안
- ID 및 접근 관리(IAM)
- 보안 평가 및 테스트
- 보안 운영
- 소프트웨어 개발 보안

경력 요구 사항

지원자는 CISSP CBK의 8개 분야 중 2개 이상에서 최소 5년간 누적된 직업 경력이 있어야 합니다. 4년제 대학 학위 또는 지역별 동등 학위를 취득하였거나, 또는 (ISC)²의 승인 리스트 내 추가 자격을 소지하였을 경우 1년의 요구 경력을 충족시킬 수 있습니다. 교육 학점으로는 1년의 경력만 인정됩니다.

CISSP가 되기 위해 요구되는 경력이 충족되지 못한 지원자는 CISSP 시험에 합격하여 (ISC)²에 채용될 수 있습니다. (ISC)²에 채용되는 경우 5년의 요구되는 경력을 쌓을 수 있도록 6년의 기간이 주어집니다. CISSP 경력 요건과 파트 타임 근로 및 인턴십을 지원하는 방법에 대한 자세한 사항은 www.isc2.org/Certifications/CISSP/experience-requirements 에서 확인하십시오.

인증

CISSP는 ANSI/ISO/IEC 표준 17024의 엄격한 요구 사항을 충족하는 정보 보안 분야의 최초 자격증입니다.

직무 과제 분석(JTA)

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

CISSP CAT 시험 정보

CISSP 시험은 영어 시험에 있어 전산화 적응 시험(CAT)을 사용합니다. 다른 모든 언어로 진행되는 CISSP 시험은 선형 시험, 고정형 시험으로 시행됩니다. CISSP CAT에 대한 자세한 사항은 www.isc2.org/certificatons/CISSP-CAT 에서 확인하십시오.

시험 시간	3시간
문항 수	100~150
문제 형식	객관식과 상급의 혁신적 문항
합격 기준	700점 이상(총점 1000점)
사용 가능한 시험 언어	영어
테스트 센터	(ISC)² Authorized PPC and PVTC Select Pearson VUE Testing Centers

CISSP CAT 시험 가중치

분야	평균
1. 보안 및 위험 관리	15%
2. 자산 보안	10%
3. 보안 아키텍처 및 엔지니어링	13%
4. 통신 및 네트워크 보안	13%
5. ID 및 접근 관리(IAM)	13%
6. 보안 평가 및 테스트	12%
7. 보안 운영	13%
8. 소프트웨어 개발 보안	11%
총:	**100%**

CISSP 선형 시험 정보

시험 시간	6시간
문항 수	250
문제 형식	객관식과 상급의 혁신적 문항
합격 기준	700점 이상(총점 1000점)
사용 가능한 시험 언어	프랑스어, 독일어, 브라질 포르투갈어, 스페인어, 일본어, 간체 중국어, 한국어
테스트 센터	(ISC)² Authorized PPC and PVTC Select Pearson VUE Testing Centers

CISSP 선형 시험 가중치

분야	가중치
1. 보안 및 위험 관리	15%
2. 자산 보안	10%
3. 보안 아키텍처 및 엔지니어링	13%
4. 통신 및 네트워크 보안	13%
5. ID 및 접근 관리(IAM)	13%
6. 보안 평가 및 테스트	12%
7. 보안 운영	13%
8. 소프트웨어 개발 보안	11%
총:	**100%**

분야 1: 보안 및 위험 관리

1.1 직업 윤리 이해, 준수 및 증진

» (ISC)² 직업 윤리 강령
» 조직 윤리 강령

1.2 보안 개념 이해 및 적용

» 기밀성, 무결성 및 가용성, 진정성 및 부인 방지

1.3 보안 거버넌스 원칙의 평가 및 적용

» 보안 기능을 사업 전략, 목표, 사명 및 목적과 연계
» 조직 프로세스(예: 인수, 매각, 거버넌스 위원회)
» 조직의 역할과 책임
» 보안 통제 프레임워크
» 상당한 주의/실사

1.4 규정 준수 요구 사항 결정

» 계약, 법률, 업계 표준 및 규제 요구 사항
» 개인 정보 보호 요구 사항

1.5 전체적인 맥락에서 정보 보안과 관련된 법률 및 규제 문제 이해

» 사이버 범죄 및 데이터 유출
» 라이선싱 및 지적 재산(IP) 요구 사항
» 수입/수출 규제
» 국경 간 데이터 흐름
» 개인 정보

1.6 조사 유형에 대한 요구 사항 이해(예: 행정, 형사, 민사, 규제, 산업 표준)

1.7 보안 정책, 표준, 절차 및 지침의 개발, 문서화 및 구현

1.8 사업 연속성(BC) 요구 사항의 식별, 분석 및 우선순위 지정

» 사업 영향 분석(BIA)
» 범위와 계획의 개발 및 문서화

1.9 인사 보안 정책 및 절차에 대한 기여 및 시행

» 지원자 심사 및 고용
» 고용 계약 및 정책
» 입사, 이직 및 퇴사 프로세스
» 공급 업체, 컨설턴트 및 계약업체 계약 및 통제
» 규정 준수 정책 요구 사항
» 개인 정보 보호 정책 요구 사항

1.10 리스크 관리의 개념 이해 및 적용

» 위협 및 취약점 식별
» 위험 평가/분석
» 위험 대응
» 대응책 선택 및 구현
» 적용 가능한 통제 유형(예: 예방, 탐지, 시정)
» 통제 평가(보안 및 개인 정보)
» 모니터링 및 측정
» 보고
» 지속적인 개선(예: 위험 성숙도 모델링)
» 위험 프레임워크

1.11 위협 모델링 개념 및 방법론의 이해 및 적용

1.12 공급망 위험 관리(SCRM) 개념 적용

» 하드웨어, 소프트웨어 및 서비스와 관련된 위험
» 제3자 평가 및 모니터링
» 최소 보안 요구 사항
» 서비스 수준 요구 사항

1.13 보안 인식, 교육 및 훈련 프로그램 수립 및 유지

» 인식과 훈련을 제시하는 방법과 기법(예: 사회 공학, 피싱, 보안 챔피언, 게임화)
» 주기적인 내용 검토
» 프로그램 효과성 평가

분야 2: 자산 보안

2.1 정보 및 자산의 식별 및 분류

» 데이터 분류
» 자산 분류

2.2 정보 및 자산 취급의 요구 사항 수립

2.3 안전한 자원 프로비저닝

» 정보 및 자산 소유권
» 자산 인벤토리(예: 유형, 무형)
» 자산 관리

2.4 데이터 수명 관리

» 데이터 역할(예: 소유자, 컨트롤러, 관리자, 프로세서, 사용자/주체)
» 데이터 수집
» 데이터 위치
» 데이터 유지관리
» 데이터 보존
» 데이터 잔류 자기
» 데이터 파괴

2.5 적절한 자산 보유 보장(예: 사용 종료(EOL), 지원 종료(EOS))

2.6 데이터 보안 통제 및 규정 준수 요구 사항 결정

» 데이터 상태(예: 사용 중, 이전 중, 휴지 중)
» 범위 지정 및 조정
» 표준 선택
» 데이터 보호 방법(예: 디지털 저작권 관리(DRM), 데이터 손실 방지(DLP), 클라우드 접근 보안 브로커(CASB))

분야 3: 보안 아키텍처 및 엔지니어링

3.1 안전한 디자인 원칙을 사용하여 엔지니어링 프로세스 연구, 구현 및 관리

- 위협 모델링
- 최소 권한
- 심층 방어
- 보안 기본값
- 안전 고장
- 업무 분리(SoD)
- 간단 명료하게(KIS)
- 제로 트러스트
- 프라이버시 바이 디자인(PbD)
- 신뢰하지만 검증
- 공동 책임 모델

3.2 보안 모델의 기본 개념 이해(예: Biba, Star Model, Bell-LaPadula)

3.3 시스템 보안 요구 사항에 따라 통제 선택

3.4 정보 시스템(IS)의 보안 기능 이해(예: 메모리 보호, 신뢰할 수 있는 플랫폼 모듈(TPM), 암호화/암호 해독)

3.5 보안 아키텍처, 설계 및 솔루션 요소의 취약성 평가 및 완화

- 클라이언트 기반 시스템
- 서버 기반 시스템
- 데이터베이스 시스템
- 암호화 시스템
- 산업 통제 시스템(ICS)
- 클라우드 기반 시스템(예: 소프트웨어형 서비스(SaaS), 서비스 형태 인프라(IaaS), 플랫폼형 서비스(PaaS))
- 분산 시스템
- 사물인터넷(IoT)
- 마이크로서비스
- 컨테이너리제이션
- 서버리스
- 임베디드 시스템
- 고성능 컴퓨팅(HPC) 시스템
- 에지 컴퓨팅 시스템
- 가상화 시스템

3.6 암호화 솔루션의 선택과 결정

- 암호화 라이프 사이클(예: 키, 알고리즘 선택)
- 암호화 방법(예: 대칭, 비대칭, 타원 곡선, 양자)
- 공개 키 기반구조(PKI)
- 키 관리 관행
- 디지털 서명 및 디지털 인증서
- 부인 방지
- 무결성(예: 해시)

3.7 암호 해독 공격 방법 이해

- 억지 기법
- 암호문만 사용
- 알려진 평문
- 빈도 분석
- 선택된 암호문
- 구현 공격
- 부채널
- 결함 제거
- 타이밍
- 중간자(MITM)
- 해시
- 커버로스 공격
- 랜섬웨어

3.8 현장 및 시설 설계에 보안 원칙 적용

3.9 현장 및 시설 보안 통제 구현

- 배선 보관함/중간 유통 시설
- 서버 룸/데이터 센터
- 미디어 저장 시설
- 증거 저장소
- 제한 구역 및 작업 구역 보안
- 유틸리티 및 난방, 통풍 및 공조(HVAC)
- 환경 문제
- 화재 예방, 탐지 및 억제
- 전원(예: 여분, 예비)

분야 4: 통신 및 네트워크 보안

4.1 네트워크 아키텍처에서 보안 설계 원칙 평가 및 구현

» 개방형 시스템간 상호 접속(OSI) 및 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP) 모델
» 인터넷 프로토콜(IP) 네트워킹(예: 인터넷 프로토콜 보안(IPSec), 인터넷 프로토콜(IP) v4/6)
» 보안 프로토콜
» 다중 프로토콜의 의미
» 수렴형 프로토콜(예: 이더넷을 통한 파이버 채널(FCoE), 인터넷 소형 컴퓨터 시스템 인터페이스(iSCSI), 음성 인터넷 프로토콜(VoIP))
» 마이크로 세분화(예: 소프트웨어 정의 네트워크(SDN), VXLAN, 캡슐화, 소프트웨어 정의 광역 네트워크(SD-WAN))
» 무선 네트워크(예: Li-Fi, Wi-Fi, 직비, 위성)
» 셀 네트워크(예: 4G, 5G)
» 콘텐츠 배포 네트워크(CDN)

4.2 안전한 네트워크 구성 요소

» 하드웨어 운영(예: 여분 전원, 보증, 지원)
» 전송 매체
» 네트워크 접근 통제(NAC) 장치
» 엔드포인트 보안

4.3 설계에 따라 안전한 통신 채널 구현

» 음성
» 멀티미디어 협업
» 원격 접속
» 데이터 통신
» 가상 네트워크
» 제3자 연결성

분야 5: ID 및 접근 관리(IAM)

5.1 자산에 대한 물리적 및 논리적 접근 통제

- 정보
- 시스템
- 장치
- 시설
- 어플리케이션

5.2 사람, 장치 및 서비스의 식별 및 인증 관리

- 신원 관리(IdM) 구현
- 단일/다중 인증(MFA)
- 책임 추적성
- 세션 관리
- 신원 등록, 입증 및 수립
- 연합 ID 관리(FIM)
- 자격 증명 관리 시스템
- 통합 인증(SSO)
- 적시생산방식(JIT)

5.3 제3자 서비스와 연합 ID

- 현장
- 클라우드
- 하이브리드

5.4 인증 메커니즘 구현 및 관리

- 역할 기반 접근 통제(RBAC)
- 역할 기반 접근 통제
- 강제적 접근 통제(MAC)
- 임의적 접근 통제(DAC)
- 속성 기반 접근 통제(ABAC)
- 위험 기반 접근 통제

5.5 신원 및 액세스 프로비저닝 수명주기 관리

- 계정 접근 리뷰(예: 사용자, 시스템, 서비스)
- 프로비저닝 및 프로비저닝 해제(예: 입사 및 이직 온/오프)
- 역할 정의(예: 새로운 역할에 배정된 사람들)
- 권한 상승(예: 관리 서비스 계정, sudo 사용, 사용 최소화)

5.6 인증 시스템 구현

- OpenID 연결(OIDC)/공개 승인(Oauth)
- 보안 접근제어 명령 생성 언어(SAML)
- Kerberos
- 원격 인증 전화 접속 사용자 서비스(RADIUS)/터미널 접속 제어기 접근 제어 시스템 플러스(TACACS+)

분야 6: 보안 평가 및 테스트

6.1 평가, 테스트 및 감사 전략 설계 및 검증

» 내부
» 외부
» 제3자

6.2 보안 통제 테스트 실시

» 취약성 평가
» 침투 테스트
» 로그 리뷰
» 통합 거래
» 코드 검토 및 테스트
» 오용 사례 테스트
» 테스트 커버리지 분석
» 인터페이스 테스트
» 침해 공격 시뮬레이션
» 규정 준수 확인

6.3 보안 프로세스 데이터 수집(예: 기술 및 관리)

» 계정 관리
» 경영 검토 및 승인
» 주요 성과 및 위험 지표
» 백업 검증 데이터
» 교육 및 인식
» 재난 복구(DR) 및 사업 연속성(BC)

6.4 시험 결과 분석 및 보고서 생성

» 교정
» 예외 취급
» 윤리 강령 공개

6.5 보안 감사 실시 또는 촉진

» 내부
» 외부
» 제3자

분야 7: 보안 운영

7.1 조사의 이해 및 지원

» 증거 수집 및 취급
» 보고 및 문서화
» 조사 기술
» 디지털 포렌식 도구, 전술 및 절차
» 아티팩트(예: 컴퓨터, 네트워크, 모바일 장치)

7.2 로깅 및 모니터링 활동 수행

» 침입 탐지 및 예방
» 보안 정보 및 이벤트 관리(SIEM)
» 지속적인 모니터링
» 송신 모니터링
» 로그 관리
» 위협 인텔리전스(예: 위협 피드, 위협 헌팅)
» 사용자 및 엔티티 행동 분석(UEBA)

7.3 구성 관리(CM) 수행(예: 프로비저닝, 기준선 설정, 자동화)

7.4 기본적인 보안 운영 개념의 적용

» 알아 두어야 할 사항/최소 권한
» 업무와 책임의 분리
» 권한 있는 계정 관리
» 직무 순환
» 서비스 수준 협약(SLAs)

7.5 자원 보호 기술 적용

» 미디어 관리
» 미디어 보호 테크닉

7.6 사고 관리 수행

» 탐지
» 응답
» 완화
» 보고
» 복구
» 교정
» 교훈

7.7 탐지 및 예방조치 시행 및 유지

- 방화벽(예: 차세대, 웹 어플리케이션, 네트워크)
- 침입 탐지 시스템(IDS) 및 침입 예방 시스템(IPS)
- 화이트리스트/블랙리스트
- 제3자 제공 보안 서비스
- 샌드박스
- 허니팟/허니넷
- 안티 맬웨어
- 머신 러닝 및 인공 지능(AI) 기반 도구

7.8 패치 및 취약점 관리 구현 및 지원

7.9 변경 관리 프로세스 이해 및 참여

7.10 복구 전략 구현

- 백업 스토리지 전략
- 복구 사이트 전략
- 다중 처리 사이트
- 시스템 복원력, 고가용성(HA), 서비스 품질(QoS) 및 내결함성

7.11 재난 복구(DR) 프로세스 구현

- 응답
- 인사
- 통신
- 평가
- 복원
- 교육 및 인식
- 교훈

7.12 재난 복구 계획(DRP) 테스트

- 재해 복구 계획 문서 검토
- 연습
- 모의 훈련
- 병렬
- 완전 중단

7.13 사업 연속성(BC) 계획 및 연습에 참여

7.14 물리적 보안 구현 및 관리

- 경계 보안 통제
- 내부 보안 통제

7.15 인력 안전과 보안 문제 제기

- 출장
- 보안 교육 및 인식
- 비상 관리
- 협박

분야 8: 소프트웨어 개발 보안

8.1 소프트웨어 개발 생애주기(SDLC)의 보안 이해 및 통합

» 개발 방법론(예: Agile, Waterfall, DevOps, DevSecOps)
» 성숙도 모델(예: 능력 성숙도 모델(CMM), 소프트웨어 보증 성숙도 모형(SAMM))
» 운영 및 유지보수
» 변경 관리
» 제품 통합 팀(IPT)

8.2 소프트웨어 개발 환경에서 보안 통제 식별 및 적용

» 프로그래밍 언어
» 라이브러리
» 도구 모음
» 통합 개발 환경(IDE)
» 런타임
» 지속적 통합과 지속적 제공(CI/CD)
» 보안 오케스트레이션, 자동화 및 응답(SOAR)
» 소프트웨어 환경설정 관리(SCM)
» 코드 저장소
» 어플리케이션 보안 테스트(예: 정적 어플리케이션 기반 보안 시험(SAST), 동적 어플리케이션 보안 테스트(DAST))

8.3 소프트웨어 보안의 효과성 평가

» 변경 사항 감사 및 로깅
» 위험 분석 및 완화

8.4 획득한 소프트웨어의 보안 영향 평가

» 상용(COTS)
» 오픈 소스
» 제3자
» 관리 서비스(예: 소프트웨어형 서비스(SaaS), 서비스 형태 인프라(IaaS), 플랫폼형 서비스(PaaS))

8.5 보안 코딩 지침 및 표준 정의 및 적용

» 소스 코드 레벨에서 보안 약점 및 취약점
» 어플리케이션 프로그래밍 인터페이스(APIs)의 보안
» 안전한 코딩 방법
» 소프트웨어 정의 보안

시험관련 추가 정보

추가 참조 사항

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

추가 참조 전체 목록은 www.isc2.org/certifications/References 에서 확인하십시오.

시험 정책 및 절차

(ISC)²는 CISSP 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: +1.866.331.ISC2 (4722)
이메일: info@isc2.org

(ISC)² Asia Pacific
전화번호: +(852) 28506951
이메일: isc2asia@isc2.org

(ISC)² EMEA
전화번호: +44 (0)203 300 1625
이메일: info-emea@isc2.org