



# Certified Information Systems Security Professional

## 자격증 시험 개요

Effective Date: April 2018



# About CISSP

CISSP (Certified Information Systems Security Professional)는 정보 보안 업계에서 국제적으로 가장 널리 인정되는 자격증입니다. CISSP는 조직의 전반적인 보안 상태를 효과적으로 설계, 운영 및 관리하기 위해 요구되는 정보 보안 전문가의 심도 있는 기술 및 관리 지식과 경험을 검증합니다.

CISSP CBK (Common Body of Knowledge)에 포함된 광범위한 주제는 정보 보안의 모든 분야와의 관련성을 보장합니다. 성공적인 지원자는 다음 8개 도메인에 관련된 능력이 입증됩니다.

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

## 경력 요구 사항

지원자는 CISSP CBK의 8개 도메인 중 2개 이상에서 최소 5년간 누적된 직업 경력이 있어야 합니다. 4년제 대학 학위 또는 지역별 동등 학위를 취득하였거나, 또는 (ISC)<sup>2</sup> 승인 리스트 내 추가 자격을 소지하였을 경우 1년의 요구 경력을 충족시킬 수 있습니다. 교육 크레딧으로는 1년의 경력만을 인정합니다.

CISSP가 되기 위해 요구되는 경력이 충족되지 못한 지원자는 CISSP 시험에 성공적으로 합격하여 Associate of (ISC)<sup>2</sup> 가 될 수 있습니다. Associate of (ISC)<sup>2</sup> 에게는 5년의 요구되는 경력을 쌓을 수 있도록 6년이 주어집니다.

## 인증

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

## 직무 과제 분석(Job Task Analysis)

(ISC)<sup>2</sup> 는 회원들을 위해 CISSP의 적합성 유지의 의무를 갖습니다. 정기적으로 수행되는 직무 과제 분석(Job Task Analysis)은 CISSP에서 정의한 직업에 종사하는 보안 전문가가 수행하는 직무/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 영역에서 테스트를 거치게 됩니다.

## CISSP CAT 시험 정보

CISSP 시험은 영어 시험에 있어 Computerized Adaptive Testing (CAT)을 적용합니다. 다른 모든 언어의 CISSP 시험은 선형 시험, 고정형 시험으로 시행됩니다. CISSP CAT에 대한 자세한 내용은 [www.isc2.org/certifications/CISSP-CAT](http://www.isc2.org/certifications/CISSP-CAT)에서 확인할 수 있습니다.

시험 시간	3 시간
문항 수	100 – 150
문제 형식	객관식 및 상급의 혁신적 문항
합격 점수	총점 1000점에서 700점 이상
시험 언어	영어
테스트 센터	(ISC) <sup>2</sup> Authorized PPC and PVTC Select Pearson VUE Testing Centers

## CISSP CAT 시험 가중치

도메인	평균 가중치
1. 보안 및 위험 관리	15%
2. 자산 보안	10%
3. 보안 아키텍처 및 엔지니어링	13%
4. 통신 및 네트워크 보안	14%
5. 신원 및 접근 관리(IAM)	13%
6. 보안 평가 및 테스트	12%
7. 보안 운영	13%
8. 소프트웨어 개발 보안	10%
Total:	100%

## CISSP 선형(Linear) 시험 정보

시험 시간	6 시간
문항 수	250
문제 형식	객관식 및 상급의 혁신적 문항
합격 기준	700점 이상 (총점 1000점)
시험 언어	프랑스어, 독일어, 브라질 포르투갈어, 스페인어, 일본어, 중국어, 한국어
테스트 센터	(ISC) <sup>2</sup> Authorized PPC and PVT Select Pearson VUE Testing Centers

## CISSP 선형(Linear) 시험 가중치

도메인	가중치
1. 보안 및 위협 관리	15%
2. 자산 보안	10%
3. 보안 아키텍처 및 엔지니어링	13%
4. 통신 및 네트워크 보안	14%
5. 신원 및 접근관리(IAM)	13%
6. 보안 평가 및 테스트	12%
7. 보안 운영	13%
8. 소프트웨어 개발 보안	10%
Total: 100%	



# Domain 1: 보안 및 위험 관리

## 1.1 기밀성, 무결성 및 가용성에 대한 개념 이해 및 적용

## 1.2 보안 거버넌스 원칙의 평가 및 적용

- » 보안 기능을 비즈니스 전략, 목표, 사명 및 목적과 연계
- » 조직 프로세스 (예 : 인수, 매각, 거버넌스위원회)
- » 조직의 역할과 책임
- » 보안 제어 프레임워크
- » 상당한 주의 / 실사

## 1.3 규정 준수 요구사항 결정

- » 계약, 법률, 업계 표준 및 규제 요구사항
- » 개인 정보 보호 요구사항

## 1.4 글로벌 맥락에서 정보 보안과 관련된 법률 및 규제 문제 이해

- » 사이버 범죄 및 데이터 유출
- » 라이선싱 및 지적재산권 요구 사항
- » 수입 / 수출 규제
- » 국경 간 데이터 흐름
- » 개인 정보 보호

## 1.5 직업 윤리 이해, 준수 및 증진

- » (ISC)<sup>2</sup> 직업 윤리 강령
- » 조직 윤리 강령

## 1.6 보안 정책, 표준, 절차 및 지침의 개발, 문서화 및 구현

## 1.7 비즈니스 연속성 (BC) 요구 사항의 식별, 분석 및 우선 순위 지정

- » 범위와 계획의 개발 및 문서화
- » 비즈니스 영향 분석 (BIA)

### 1.8 인사 보안 정책 및 절차에 대한 기여 및 시행

- » 후보자 선발 및 채용
- » 고용 계약 및 정책
- » 입사 및 퇴사 프로세스
- » 공급 업체, 컨설턴트 및 계약직 계약 및 통제
- » 규정 준수 정책 요구 사항
- » 개인 정보 보호 정책 요구 사항

### 1.9 리스크 관리 개념 이해 및 적용

- » 위협 및 취약점 식별
- » 위협 평가 / 분석
- » 위협 대응
- » 대응책 선택 및 구현
- » 적용 가능한 통제 유형 (예: 예방, 탐지, 교정)
- » 보안 통제 평가(SCA)
- » 모니터링 및 측정
- » 자산 평가
- » 보고
- » 지속적인 개선
- » 위험 요소 프레임워크

### 1.10 위협 모델링 개념 및 방법론 이해 및 적용

- » 위협 모델링 방법론
- » 위협 모델링 개념

### 1.11 리스크 기반 경영 개념을 공급망에 적용

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

### 1.12 보안 인식, 교육 및 훈련 프로그램 수립 및 유지

- » 인식과 훈련을 제시하는 방법과 기법
- » 주기적인 내용 검토
- » 프로그램 효과성 평가



## Domain 2: 자산 보안

### 2.1 정보 및 자산 식별 및 분류

- » 데이터 분류
- » 자산 분류

### 2.2 정보 및 자산 소유권 결정 및 유지

### 2.3 개인 정보 보호

- » 데이터 소유자
- » 데이터 처리자
- » 데이터 흔적 (잔류 자기)
- » 수집 제한

### 2.4 적절한 자산 보유 보장

### 2.5 데이터 보안 통제 결정

- » 데이터 상태 이해
- » 범위 지정 및 개조 (Tailoring)
- » 표준 선택
- » 데이터 보호 방법

### 2.6 정보 및 자산 처리 요구 사항 수립



## Domain 3: 보안 아키텍처 및 엔지니어링

- 3.1 안전한 디자인 원칙을 사용하여 엔지니어링 프로세스 구현 및 관리
- 3.2 보안 모델의 기본 개념 이해
- 3.3 시스템 보안 요구 사항에 따라 통제 선택
- 3.4 정보 보호 시스템의 보안 기능 이해 (예: 메모리 보호, TPM (신뢰할 수 있는 플랫폼 모듈), 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
  - » 산업용 제어 시스템 (ICS)
  - » 클라우드 기반 시스템
  - » 분산 시스템
  - » 사물 인터넷 (IoT)
- 3.6 웹 기반 시스템의 취약성 평가 및 완화
- 3.7 모바일 시스템의 취약성 평가 및 완화
- 3.8 임베디드 장치의 취약성 평가 및 완화
- 3.9 암호화 적용
  - » 암호화 라이프 사이클 (예: 키 관리, 알고리즘 선택)
  - » 암호화 방법 (예: 대칭, 비대칭, 타원 곡선)
  - » 공용 키 인프라 (PKI)
  - » 키 관리 프랙티스
  - » 디지털 서명
  - » 부인 방지
  - » 무결성 (예: 해시)
  - » 암호 해독 공격 방법 이해
  - » 디지털 권한 관리 (DRM)
- 3.10 현장 및 시설 설계에 보안 원칙 적용



### 3.11 현장 및 시설 보안 통제 구현

- » 배선 보관함 / 중간 유통 시설
- » 서버 룸 / 데이터 센터
- » 미디어 저장 시설
- » 증거 저장
- » 제한 구역 및 작업 구역 보안
- » 유틸리티 및 난방, 환기 및 공조 (HVAC)
- » 환경 문제
- » 화재 예방, 감지 및 억제



## Domain 4: 통신 및 네트워크 보안

### 4.1 네트워크 아키텍처에서 보안 설계 원칙 구현

- » OSI (Open System Interconnection) 및 TCP / IP (Transmission Control Protocol / Internet Protocol) 모델
- » 인터넷 프로토콜 (IP) 네트워킹
- » 다중 프로토콜의 의미
- » 수렴형 프로토콜
- » 소프트웨어 정의 네트워크
- » 무선 네트워크

### 4.2 안전한 네트워크 구성 요소

- » 하드웨어 운영
- » 전송 매체
- » 네트워크 액세스 제어 (NAC) 장치
- » 엔드포인트 보안
- » 콘텐츠 배포 네트워크

### 4.3 설계에 따라 안전한 통신 채널 구현

- » 음성
- » 멀티미디어 협업
- » 원격 액세스
- » 데이터 통신
- » 가상 네트워크



## Domain 5: 신원 및 접근 관리 (IAM)

### 5.1 자산에 대한 물리적 및 논리적 접근 통제

- » 정보
- » 시스템
- » 장치
- » 시설

### 5.2 사람, 장치 및 서비스의 식별 및 인증 관리

- » 신원 관리 구현
- » 단일 / 다중 요소 인증
- » 책임 추적성
- » 세션 관리
- » 신원 등록 및 인증
- » FIM (Federated Identity Management)
- » 자격 관리 시스템

### 5.3 제 3 자 서비스로서의 신원 통합

- » 현장 (On-premise)
- » 클라우드
- » 연합 (Federated)

### 5.4 인증 메커니즘 구현 및 관리

- » 역할 기반 접근 통제 (RBAC)
- » 규칙 기반 접근 통제
- » 필수 접근 통제 (MAC)
- » 임의 접근 통제 (DAC)
- » 속성 기반 접근 통제 (ABAC)

### 5.5 신원 및 액세스 프로비저닝 수명주기 관리

- » 사용자 액세스 검토
- » 시스템 계정 액세스 검토
- » 프로비저닝 및 프로비저닝 해제



## Domain 6: 보안 평가 및 테스트

### 6.1 평가, 테스트 및 감사 전략 설계 및 검증

- » 내부
- » 외부
- » 제 3 자

### 6.2 보안 통제 테스트 실시

- » 취약점 평가
- » 침투 테스트
- » 로그 리뷰
- » 통합 거래
- » 코드 검토 및 테스트
- » 오용 사례 테스트
- » 테스트 커버리지 분석
- » 인터페이스 테스트

### 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
- » 재해 복구 (DR) 및 비즈니스 연속성 (BC)

### 6.4 시험 결과 분석 및 보고서 생성

### 6.5 보안 감사 실시 또는 촉진

- » 내부
- » 외부
- » 제 3 자



## Domain 7: 보안 운영

### 7.1 조사의 이해 및 지원

- » 증거 수집 및 처리
- » 보고 및 문서
- » 조사 기술
- » 디지털 포렌식 도구, 전술 및 절차

### 7.2 조사 유형에 대한 요구 사항 이해

- » 행정
- » 범죄자
- » 시민
- » 규제
- » 산업 표준

### 7.3 로깅 및 모니터링 활동 수행

- » 침입 탐지 및 예방
- » 보안 정보 및 이벤트 관리 (SIEM)
- » 지속적인 모니터링
- » 출구 모니터링

### 7.4 안전한 리소스 프로비저닝

- » 자산 인벤토리
- » 자산 관리
- » 구성 관리

### 7.5 기본적인 보안 운영 개념의 이해 및 적용

- » 알아 두어야 할 사항 / 최소 권한
- » 직무와 책임의 분리
- » 특권 계정 관리
- » 직무 순환
- » 정보 수명 주기
- » 서비스 수준 계약 (SLA)

### 7.6 자원 보호 기술 적용

- » 미디어 관리
- » 하드웨어 및 소프트웨어 자산 관리

## 7.7 사고 관리 수행

- » 탐지
- » 응답
- » 완화
- » 보고
- » 복구
- » 교정
- » 교훈

## 7.8 탐지 및 예방조치를 시행하고 유지

- » 방화벽
- » 침입 탐지 및 방지 시스템
- » 화이트리스트 / 블랙리스트
- » 제3자 제공 보안 서비스
- » 샌드박스
- » 허니팟 / 허니넷
- » 안티 맬웨어

## 7.9 패치 및 취약점 관리 구현 및 지원

## 7.10 변경 관리 프로세스 이해 및 참여

## 7.11 복구 전략 구현

- » 백업 스토리지 전략
- » 복구 사이트 전략
- » 다중 처리 사이트
- » 시스템 복원력, 고 가용성, QoS 및 내 결합성

## 7.12 재해 복구 (DR) 프로세스 구현

- » 응답
- » 인사
- » 커뮤니케이션
- » 평가
- » 복원
- » 교육 및 인지도

## 7.13 재해 복구 계획 (DRP) 테스트

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

## 7.14 비즈니스 연속성 (BC) 계획 및 연습에 참여

## 7.15 물리적 보안 구현 및 관리

- » 경계 보안 통제
- » 내부 보안 통제

## 7.16 인력 안전과 보안 문제를 제기

- » 여행
- » 보안 교육 및 인지도
- » 비상 관리
- » 협박



## 영역 8: 소프트웨어 개발 보안

### 8.1 소프트웨어 개발 라이프사이클(SDLC)에서의 보안을 이해하고 통합

- » 개발 방법론
- » 성숙도 모델
- » 운영 및 유지보수
- » 변경 관리
- » 통합 제품 팀

### 8.2 개발 환경에서 보안 통제 식별 및 적용

- » 소프트웨어 환경의 보안
- » 보안 코딩 측면에서의 구성 관리
- » 코드 저장소 보안

### 8.3 소프트웨어 보안의 효과성 평가

- » 변경 사항 감사 및 로깅
- » 위험 분석 및 완화

### 8.4 획득한 소프트웨어의 보안 영향 평가

### 8.5 보안 코딩 지침 및 표준 정의 및 적용

- » 소스 코드 레벨에서 보안 약점 및 취약점
- » 어플리케이션 프로그래밍 인터페이스의 보안
- » 안전한 코딩 방법

# 시험관련 추가 정보

## 추가 참조 사항

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

추가 참조 전체 목록은 다음 사이트에 있습니다.

[www.isc2.org/certifications/References](http://www.isc2.org/certifications/References).

## 시험 정책 및 절차

(ISC)<sup>2</sup>는 CISSP 지원자가 시험에 등록하기에 앞서 시험 정책 및 절차를 검토 할 것을 권장합니다. 다음의 중요한 정보에 대한 종합적인 내용은 [www.isc2.org/Register-for-Exam](http://www.isc2.org/Register-for-Exam)에서 확인하십시오.

## 법률 정보

(ISC)<sup>2</sup>의 법률 정책과 관련된 질문은 [legal@isc2.org](mailto:legal@isc2.org) (ISC)<sup>2</sup> 법률 부서에 문의하십시오.

## 문의사항 연락처

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

(ISC)<sup>2</sup> Americas  
Tel: +1.866.331.ISC2 (4722)  
Email: [info@isc2.org](mailto:info@isc2.org)

(ISC)<sup>2</sup> Asia Pacific  
Tel: +(852) 28506951  
Email: [isc2asia@isc2.org](mailto:isc2asia@isc2.org)

(ISC)<sup>2</sup> EMEA  
Tel: +44 (0)203 300 1625  
Email: [info-emea@isc2.org](mailto:info-emea@isc2.org)