Certified in Cybersecurity

An (ISC)² Certification

인증 시험 개요

발효일: 2022년 8월 29일

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

사이버 보안 인증 시험 자격에 관하여

사이버 보안 인증(CC)은 고용주에게 귀하가 초급 또는 중급 사이버 보안 역할에 필요한 기본 지식, 기술, 역량을 갖추고 있음을 증명합니다. 이 자격은 기본 보안 모범 사례, 정책 및 절차에 대한 이해는 물론 더 많은 것을 배우고 직장에서 성장하려는 의지와 역량을 나타냅니다.

시험에서는 다섯 가지 영역을 다룹니다.

- 보안 원칙
- 사업 연속성(BC), 재해 복구(DR), 사고 대응 개념
- 접근 통제 개념
- 네트워크 보안
- 보안 운영

경력 요구 사항

시험에 응시하기 위한 특정 전제조건은 없습니다. 하지만 응시자가 기본 IT 지식을 보유하는 것이 권장됩니다. 사이버 보안 분야의 업무 경험이나 공식적인 졸업장/학위는 필요하지 않습니다. 응시자 경력의 다음 단계에서 (ISC)² 전문가 수준 인증을 획득하기 위한 상황에서는 현장 경험이 필요합니다.

직무 과제 분석(JTA)

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

CC 시험 정보

시험 시간	2시간
문항 수	100
문항 형식	선다형 문제
합격 기준	1000점 만점에 700점
시험 제공 언어	영어, 한국어, 중국어, 일본어, 독일어, 스페인어
테스트 센터	Pearson VUE 테스트 센터

CC 시험 가중치

도메인	평균 가중치
1. 보안 원칙	26%
2. 사업 연속성(BC), 재해 복구(DR) 및 사고 대응 개념	10%
3. 접근 통제 개념	22%
4. 네트워크 보안	24%
5. 보안 운영	18%
총:	**100%**

도메인 1: 보안 원칙

1.1 정보 보증에 관한 보안 개념 이해

» 기밀성
» 무결성
» 가용성
» 인증(예: 인증 방법, 다중 인증(MFA))
» 부인 방지
» 개인 정보 보호

1.2 위험 관리 프로세스 이해

» 위험 관리(예: 위험 우선순위, 위험 감수도)
» 위험 식별, 평가 및 처리

1.3 보안 통제 이해

» 기술적 통제
» 관리적 통제
» 물리적 통제

1.4 (ISC)² 윤리 강령 이해

» 전문가 행동 강령

1.5 거버넌스 프로세스 이해

» 정책
» 절차
» 표준
» 규제 및 법률

도메인 2:
사업 연속성(BC), 재해 복구(DR) 및 사고 대응 개념

2.1 사업 연속성(BC) 이해

» 목적
» 중요성
» 구성 요소

2.2 재해 복구(DR) 이해

» 목적
» 중요성
» 구성 요소

2.3 사고 대응 이해

» 목적
» 중요성
» 구성 요소

도메인 3:
접근 통제 개념

3.1 물리적 접근 통제 이해

» 물리적 보안 통제(예: 배지 시스템, 게이트 입장, 환경 디자인)
» 모니터링(예: 경비원, 폐쇄회로 TV(CCTV), 경보 시스템, 로그)
» 승인된 직원과 승인되지 않은 직원

3.2 논리적 접근 통제 이해

» 최소 권한의 원칙
» 직무 분리
» 임의 접근 통제(DAC)
» 강제 접근 통제(MAC)
» 역할 기반 접근 통제(RBAC)

도메인 4: 네트워크 보안

4.1 컴퓨터 네트워킹 이해

» 네트워크 (예: 개방형 시스템 간 상호 접속(OSI) 모델, 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP) 모델, 인터넷 프로토콜 버전 4(IPv4), 인터넷 프로토콜 버전 6(IPv6), WiFi)

» 포트

» 어플리케이션

4.2 네트워크 위협 및 공격 이해

» 위협 유형(예: 분산 서비스 거부(DDoS), 바이러스, 웜, 트로이 목마, 중간자(MITM), 부채널)

» 식별(예: 침입 탐지 시스템(IDS), 호스트 기반 침입 탐지 시스템(HIDS), 네트워크 침입 탐지 시스템(NIDS))

» 예방(예: 바이러스 백신, 검사, 방화벽, 침입 방지 시스템(IPS))

4.3 네트워크 보안 인프라 이해

» 사내(예: 전력, 데이터 센터/클로젯, 공기조화기술(HVAC), 환경, 화재 진압, 이중화, 양해 각서(MOU)/계약 각서(MOA))

» 설계(예: 네트워크 분할(비무장지대(DMZ), 가상 근거리 통신망(VLAN), 가상 사설망(VPN), 마이크로 세그멘테이션), 심층 방어, 네트워크 접근 통제(NAC)(임베디드 시스템용 세그멘테이션, 사물인터넷(IoT))

» 클라우드(예: 서비스 수준 계약(SLA), 관리형 서비스 공급자(MSP), 서비스형 소프트웨어(SaaS), 서비스형 인프라(IaaS), 서비스형 플랫폼(PaaS), 하이브리드)

도메인 5:
보안 운영

5.1 데이터 보안 이해

» 암호화(예: 대칭, 비대칭, 해싱)
» 데이터 처리(예: 파기, 보존, 분류, 라벨링)
» 보안 이벤트 로깅 및 모니터링

5.2 시스템 강화 이해

» 구성 관리(예: 기준선, 업데이트, 패치)

5.3 보안 정책 베스트프랙티스 이해

» 데이터 처리 정책
» 암호 정책
» 허용되는 사용 정책(AUP)
» 개인용 디바이스를 업무에 사용(BYOD)하는 정책
» 변경 관리 정책(예: 문서화, 승인, 롤백)
» 개인 정보 보호 정책

5.4 보안 인식 교육 이해

» 목적/개념(예: 사회 공학, 암호 보호)
» 중요성

추가 시험 정보

시험 정책 및 절차

(ISC)²는 사이버 보안 인증 응시자가 시험에 등록하기에 앞서 시험 정책 및 절차를 검토할 것을 권장합니다. 다음의 중요한 정보에 대한 종합적인 내용은 www.isc2.org/Register-for-Exam에서 확인하십시오.

법률 정보

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

질문이 있나요?

해당 지역의 (ISC)² 시험 응시자 서비스에 문의할 수 있습니다.

미국
전화 : +1-866-331-ISC2 (4722)
이메일 : info@isc2.org

아시아 태평양
전화 : +852-5803-5662
이메일 : isc2asia@isc2.org

유럽, 중동 및 아프리카
전화 : +44-203-960-7800
이메일 : info-emea@isc2.org