

KCA연구2023-

# 정보보호 분야 공인민간자격 발굴 및 운영에 관한 연구

(최종보고서)

2023 . 12 . 20 .

한국방송통신전파진흥원

연구수행기관 : 한국정보보호학회

이 보고서는 한국방송통신전파진흥원의 재정지원으로 이루어졌으며, 보고서 내용은 연구자의 견해이며 한국방송통신전파진흥원의 공식 입장과 다를 수 있습니다.

# 정보보호 분야 공인민간자격 발굴 및 운영에 관한 연구

(최종보고서)

2023 . 12 . 20.

한국방송통신전파진흥원

연구수행기관 : 한국정보보호학회



# 제 출 문

한국방송통신전파진흥원장 귀하

본 보고서를 정보보호 분야 공인민간자격 발굴 및 운영에 관한 연구의 최종연구보고서로 제출합니다.

2023 년 12 월 20 일

수탁기관 : 한국정보보호학회

연구책임자 : 김태성

참여연구원 : 유진호, 조일형, 전효정



# 요 약 문

## 1. 제 목

- 정보보호 분야 공인민간자격 발굴 및 운영에 관한 연구

## 2. 연구의 목적 및 중요성

### 1) 연구의 목적

- 경제·사회 분야의 디지털 전환과 사이버보안 역량에 적합한 자격 신설 필요
  - 디지털 전환의 성공을 위한 사이버보안 역량이 요구되며, 숙련된 사이버보안 인력 검증 및 사이버보안 인식을 위한 자격(2종) 신설 필요
- 정보보호 인력양성 지원·확대 및 잠재수요의 선제적 대응 필요
  - 정보보호 인력 10만 양성 지원 및 사이버 위협에 즉시 대응 가능한 보안 분야 기획·위험평가 수행 전문자격이 요구되며, 해당 분야 잠재수요 대응 및 진입을 위한 보안 지식·역량 검증 수단이 필요

### 2) 연구의 중요성

- 정보보호 분야의 지식 및 기술을 갖춘 전문인력에 대한 수요는 앞으로도 계속 증가할 것. 다만, 정보보호 지식 및 기술의 범주가 매우 광범위해질 것이며. 이의 전문성의 정도를 평가하고 인정해 줄 수 있는 수단이 필요
  - CISO(정보보호최고책임자)/CPO(개인정보 보호책임자)로서 성장할 정도의 전문적인 지식 및 기술을 갖춘 인력도 필요하지만, 정보보호의 전산업·전사회 내재화로 인해 기초 수준의 인력도 광범위하게 필요
  - 따라서, 지능정보사회로 진입하고 있는 현시점에서 정보보호 전문성을 평가하고 증명할 수 있는 체계적이고 전문성 있는 자격제도의 마련이 필요

- 민간자격제도는 국가자격 외의 분야에서 공인받지 못하는 개인의 지식과 기술 등을 객관적으로 평가하여 자격을 부여하여 국민의 평생직업능력개발을 장려하기 위하여 도입됨
- 민간자격을 통해 자격의 취득을 위하여 교육 또는 학습에 참여가 늘어날 수 있으며, 이는 국가적으로 평생교육을 확대할 기회로 활용할 수 있음

### 3. 연구의 내용 및 범위

연구의 내용	범위
공인민간자격 발굴 및 운영(안) 수립	사이버위험 대응관리 전문가 자격 발굴, 사이버위험 역량 검정평가 운영 등을 위한 발굴·운영(안) 수립 ※2022년 KCA 연구보고서[정보보호분야 검정체계 개선방안] 참조
공인민간자격 등록방안 마련	자격기본법에 근거하여 전문가 자격 및 검정평가 등 2종 등록을 위한 자격 직무내용·검정방법 등 전반적 기술사항 마련 ※유사분야 직무내용의 포섭/배제 타당성 및 차별성 제시
신규 자격제도를 위한 문제개발	신규 자격·평가 운영을 위한 시험 문제 개발(1회의 5배수 이상) ※시험문제 개발·심사 방법은 KCA 검정관리운영규칙을 적용
신규 자격제도의 활성화 방안 도출	신규 자격·평가 활성화 및 응시자 확보 방안 도출
공청회 개최	해당분야 전문가(20인 이상) 의견수렴 및 홍보실시

### 4. 연구 결과

#### Ⅰ 공인민간자격 발굴 및 운영 방안 수립

- 2종 민간자격에 대해, 신규 개발의 필요성과 향후 운영방안 검토
- 정부는 현재 디지털 인재양성 종합방안(2022.8. 디지털 인재 100만 양성)과 사이버 10만 인재 양성 등을 추진 중. 전문인력부터 일반 기초소양을 갖춘 인력까지 전주기적 인재 양성을 위해 노력 중
- 국내 정보보호 시장(산업)이 영세하여 전문성 확보를 위한 별도의 노력이 필요한 직무임에도 불구하고 정보보호 직업만의 인센티브가 없기에 그만큼 관련 자격제도를 준비할 수요도 없는 것으로 보임

- 민간자격을 통해 자격의 취득을 위하여 교육 또는 학습에 참여가 늘어날 수 있으며, 이는 국가적으로 평생교육을 확대할 기회로 활용할 수 있음
- 현재 국내에서 운영 중인 정보보호 분야(특히, 관리적 정보보호)의 전문 자격제도로는 국가 공인자격 정보보안기사(산업기사 별도)가 있음
  - 정보보안기사의 경우, 4년제 대학 재학생이 취득하기에는 어렵고,
  - 검정 항목이 정보보안 관리 및 컴플라이언스부터 시스템/네트워크 보안 관리, 어플리케이션 보안까지 전반을 다루기에 범주가 너무 넓고, 관리적 정보보안에 특화된 자격도 아니며, 위험관리는 하위 세세항목의 하나로만 포함

< 정보보호 관련 신규 민간자격 발굴 (2종) >

자격명	사이버위험관리전문가 Cyber Risk Management Specialist (CRMS)	사이버보안수학능력평가 Cyber Literacy Generalist (CLG)
등급	등급 없음	등급 없음
검정기준	사이버위험관리 전문가로서 갖추어야 할 지식에 대한 검정과 실무에 적응할 수 있는 능력을 검정	사이버보안 관련 기초지식의 습득 정도를 검정
직무내용	조직의 정보자산을 식별하고 적절한 보안대책(통제방안)을 구현하여 조직이 감내할만한 수준으로 위험을 관리하고, 경영진에게 보안 위험관리(분석·평가 포함)를 설명하고 설득할 수 있다.	국가직무능력표준의 「정보보호관리·운영」과 「개인정보보호관리·운영」에 해당하는 지식 및 기술에 대한 기초소양을 측정한다.
검정방법	필기 : 80문항, 객관식 택일형 실기 : 5문항, 필답형	필기 : 80문항, 객관식 택일형
응시자격	4년제 대학 졸업자 또는 졸업예정자 (전공 무관, 경력자의 경우 직무 분야 무관) 및 이에 상응하는 조건	나이·학력·전공·실무경력 제한 없음
시험시간	필기 : 120분 실기 : 90분	필기 : 120분
합격기준	필기 : 과목별 40점 이상, 전체 60점 이상 실기 : 과목 통합 60점 이상	수준 평가 (800점 만점)
검정 수수료	필기 : 100,000원 (*재학생 50% 할인) 실기 : 100,000원	필기 : 30,000원
자격증 발급비	10,000원 ※온라인 무료 다운로드	10,000원 ※온라인 무료 다운로드

- 실제 정보보호 실무를 함에 있어, 조직 내 거버넌스 체계의 안정성 확보와 즉각적인 사고대응을 위해서는 위험관리 체계가 잡혀 있어야 하며, 실무자들은 충분히 훈련되어 있어야 함
  - 실질적으로, 위험 관리 및 평가는 정보보안 관리의 핵심 업무이자 숙련도를 요하는 업무이며, 전반적인 정보보안 관리 역량 평가에 필수적인 항목
  - 전산·IT·소프트웨어 등의 업무와는 차별화되면서, 정보보호 관리 업무 전반을 포괄적으로 커버할 수 있고, 보안 관리 업무에 관심있는 인력에게 필요한 자격제도 개설 필요
- 현재 국내 자격 중에는 정보보호에 관심을 가지고 기초 지식을 쌓고 평가받기를 원하는 수준의 초급자역량을 검증할 수 있는 자격제도 없음
  - 초보자들을 위한 자격제도는 정보보호 분야의 관심을 높이거나, 자신이 가진 관심이 실제 업무역량 향상을 위한 밑거름이 될만한지 가늠할 수 있는 잣대가 됨
  - 개인의 정보보호 리터러시 수준을 검증할 수 있는 자격제도가 있다면 정보보호에 대한 관심도를 높이고 자신의 수준을 점검해가며 학습 단계를 높이고, 나아가 직업으로까지 고려할 수 있는 직무 로드맵을 수립하는 데에는 도움을 줄 수 있을 것

## ② 공인민간자격 등록방안 마련 및 문제 출제/검수

- 민간자격관리운영규정 작성 [한국직업능력개발원 (2023), 민간자격 등록신청 편람(매뉴얼) 기준]
  - 검정기준, 검정과목, 검정방법, 응시자격 등을 상세화하여, 운영규정에 포함
  - 시험문제 출제 및 관리 전반에 관한 사항 상세화하여, 운영규정에 포함
- 2개 자격별로 출제기준 작성(전문가 검토 진행), 2개 민간자격 각 80문항의 5배수 출제
  - 1회분(80문항)의 5배수 출제. 10월 말 출제 완료하고, 11월~ 12월 초 검수 진행

## ③ 활성화 방안 도출

- 공청회 개최 : 계획 중인 신규 민간자격 운영방안을 설명하고, 전문가 의견 수렴
- 정보보호 분야 산/학/연의 의견을 수렴하여, 민간 자격제도 활성화 방안 도출

## 5. 활용에 대한 건의

- 다가오는 지능정보사회의 사이버보안 보장을 위한 정보보호 인력 양성 및 교육에 활용

## 6. 기 대 효 과

- 특화된 자격제도의 운영을 통해 정보보호 분야 전문인력 확보에 기여하여, 전방위적인 사이버 위협 대응체계 구축과 디지털 전환 가속화를 측면 지원

	전문적 특화	포용적 확대
사이버 위협 대응	경제·사회·산업 현장의 사이버 위협에 신속하고 전문적으로 대응할 역량을 검증 [정보보호 위협관리 특화 역량(질적 심화) 확보]	일반인(정보보호 및 관련 분야 전공자)의 정보보호에 대한 잠재적인 진로 가이드 [정보보호 리터러시 검증(양적 확대)]
자격 통합	기존 유사 민간자격 직무능력 포섭 및 통합을 통해 국방·행정·의료·산업 등 모든 분야에서 활용 가능 [모든 분야의 정보보호 문제를 해결할 수 있는 통섭형 인력 양성 기반]	초중고·일반인을 위한 디지털 소양 수준을 검증하여, 대국민 사이버 리터러시 함양에 기여 [일상적인 생활 및 사회·경제 활동 전 분야에서 정보보호가 수반되어야 함을 인식]

# 목 차

<b>제 1 장 연구의 개요</b> .....	1
제 1 절 연구의 목적 .....	1
제 2 절 연구의 방법 .....	7
제 3 절 추진계획 대비 실적 진도 .....	8
<b>제 2 장 공인민간자격 발굴 및 운영 방안</b> .....	9
제 1 절 국내외 정보보호 관련 자격제도 현황 .....	9
1. 국내 정보보호 관련 국가공인 자격제도 .....	9
2. 국내 정보보호 관련 민간 자격제도 .....	23
3. 국외 정보보호 관련 자격제도 .....	37
제 2 절 정보보호 관련 신규 민간자격 발굴 .....	45
1. 신규 민간자격 발굴 결과 .....	45
2. 국가직무능력표준과의 관계 .....	49
3. 관련 학과/전공 및 인력 수요 규모 .....	52
제 3 절 공인민간자격 등록방안 .....	61
제 4 절 민간자격 운영을 위한 시험문제 개발 .....	87
<b>제 3 장 공인민간자격 활성화 방안</b> .....	89
제 1 절 활성화 방안 .....	89
제 2 절 공청회 .....	91

# 표 목 차

<표 1-1> 연구의 추진일정 .....	8
<표 2-1> 2022년 운영기관별 국가기술자격 시행 현황 .....	9
<표 2-2> 국가기술자격 시행기관 현황 : 2022년 말 기준 .....	10
<표 2-3> 국가기술자격의 직무분야 및 국가기술자격의 종목 (정보기술 부문) .....	11
<표 2-4> 국가기술자격의 응시자 및 합격률 추이 (정보기술 부문) .....	12
<표 2-5> 정보보안기사 시험과목 .....	14
<표 2-6> 빅데이터분석기사 출제기준(필기) .....	16
<표 2-7> 빅데이터분석기사 과목별 주요 항목(필기) .....	16
<표 2-8> 빅데이터분석기사 시험과목(필기) .....	17
<표 2-9> 빅데이터분석기사 출제기준(실기) .....	18
<표 2-10> 빅데이터분석기사 과목별 주요 항목(실기) .....	18
<표 2-11> 정보처리기사 시험과목 .....	20
<표 2-12> 정보처리기사 시험과목(필기) .....	21
<표 2-13> 정보처리기사 시험과목(실기) .....	22
<표 2-14> 공인 민간자격 검색 결과 (보호 or 보안) .....	23
<표 2-15> 등록 민간자격 검색 결과 중 응시자수 1명 이상 자격 (보안 분야) .....	23
<표 2-16> 개인정보관리사 과목별 문항 및 합격기준 .....	25
<표 2-17> 블록체인관리사 응시자격 .....	26
<표 2-18> 블록체인관리사 검정과목 .....	27
<표 2-19> 인터넷보안 전문가 검정료 .....	28
<표 2-20> 인터넷보안 전문가 과목별 문항 및 합격기준 .....	28
<표 2-21> 해킹보안 전문가 과목별 문항 및 합격 기준 .....	29

<표 2-22> 해킹보안 전문가 응시자격 .....	30
<표 2-23> 개인정보보호사 검정내용 .....	31
<표 2-24> 금융보안관리사 교육과정 .....	32
<표 2-25> 금융보안관리사 자격시험 .....	32
<표 2-26> 정보보안관제사 시험 과목 및 방법 .....	33
<표 2-27> 정보보안관제사 응시자격 .....	34
<표 2-28> 디지털포렌식전문가 시험 과목 및 방법 (1급) .....	35
<표 2-29> 디지털포렌식전문가 시험 과목 및 방법 (2급) .....	36
<표 2-30> 미국 내 구인구직사이트에서의 자격증 검색 건수 (22년 12월) .....	37
<표 2-31> 국외 주요 정보보호 분야 자격제도(관리적 정보보호) 현황 .....	39
<표 2-32> ISC2 운영 자격증 .....	42
<표 2-33> ISACA 운영 자격증 .....	44
<표 2-34> 기존 정보보호 분야 자격제도의 포지셔닝 : 관리적 정보보호 부문 .....	45
<표 2-35> 한국직무능력표준(NCS) 직무능력단위 : 정보보호관리·운영 .....	49
<표 2-36> 한국직무능력표준(NCS) 직무능력단위 : 개인정보보호 .....	50
<표 3-37> 한국직무능력표준(NCS) 직무능력단위와 신규 민간자격과의 관계 .....	51
<표 2-38> 2022년 국내 4년제 대학 정보보호 관련 학과 개설 현황 .....	52
<표 2-39> 2022년 국내 4년제 대학 정보보호 관련 학과의 CRMS 관련 교과목 .....	54
<표 2-40> 국내 정보보호산업체에 종사하는 정보보안 인력 현황 (직무별) .....	58
<표 2-41> 국내 정보보호산업체에 종사하는 정보보안 인력 현황 (경력년수별) .....	58
<표 2-42> 정보보호 관련 신규 민간자격 2종 개요 .....	61
<표 2-43> 검정 수수료 설정 시 참고자료 .....	62

# 그림 목 차

<그림 1-1> 정보보호 담당자가 업무 변경을 희망하는 이유 .....	2
<그림 1-2> 디지털 인재양성 종합방안(2022)의 디지털 인재 정의 .....	3
<그림 2-1> 직무별 정보보호 인력 현황 (단위 : %) .....	59
<그림 2-2> 2022년 소프트웨어 개발 및 제작업 인력 현황 (상용 종사자) .....	60
<그림 2-3> 회수한 출제문제 예시 .....	87
<그림 2-4> 회수한 검수의견서 예시 .....	88
<그림 3-1> 공인민간자격 활성화 방안 .....	89
<그림 3-2> CRMS와 다른 자격제도와 차별성 .....	90
<그림 3-3> 공청회 - 연구진 발제 .....	91
<그림 3-4> 공청회 - 토론 및 질의응답 .....	92



# 제 1 장 연구의 개요

## 제 1 절 연구의 목적

- Forbes(2022)<sup>1)2)</sup>는 현재 기업들이 사활을 걸고 추진하고 있는 디지털 전환의 진정한 성공을 위해서는 사이버보안이 우선 확보되어야 한다고 주장
  - 사이버보안의 안정성을 보장할 수 있는 기반을 마련하지 않고 선불리 디지털화를 추진하게 되면, 데이터 유출 등의 사고를 방지할 수 없어 기업의 영속성을 보장할 수 없음
  - 기업의 사업목적과 사이버보안 활동을 일치시켜야 하기에 CISO의 역할이 중요하다고도 역설
- ISC2는 ‘사이버보안 인력 연구보고서(Cybersecurity Workforce Study 2022)’를 통해, 전세계 사이버보안 분야 종사인력의 규모를 470만 명으로 추정<sup>3)</sup>
  - 지금까지 연구 결과 중 최대 규모이지만, 여전히 부족하다고 평가
  - 점점 더 복잡해지는 현대의 위협에 대응하여 전 산업영역에서 기업(기관)들이 필요하다고 느끼는 인력의 규모 대비 부족인력의 규모는 340만 명이기 때문 (실제 고용규모가 아닌, 필요하다고 생각하는 이상적인 규모)
- 오늘날 정보보호의 역할은 단순히 정보인프라나 IT 자산을 보호하는 데에 그치지 않고 기업의 비즈니스 전체에 영향을 미치며(Shahim, 2021<sup>4)</sup>), 정보보호가 제대로 이루어지기 위해서는 정보보호 전문인력의 역할이 중요

1) <https://www.forbes.com/sites/forbestechcouncil/2022/06/09/why-cybersecurity-is-the-springboard-for-successful-digital-transformation/?sh=15a765f462cb>

2) <https://www.forbes.com/sites/forbestechcouncil/2022/05/23/taking-the-next-step-in-digital-transformation-modernizing-cybersecurity/?sh=d2c917d2f63b>

3) <https://www.isc2.org/research>

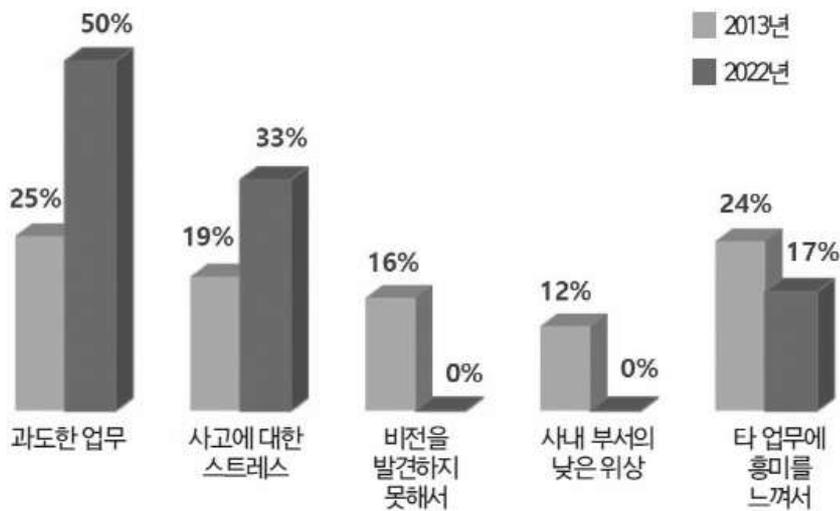
4) Shahim, A., (2021), “Security of the digital transformation,” Computers & Security, 108, Article 102345.

○ 인력은 자신이 가진 지식 및 기술의 수준과 보유한 자격증 등을 인력시장에서 우위를 차지할 수 있는 강력한 신호로 해석 (Spence, 1973; Spence, 1976; Connelly et al., 2011<sup>5)</sup>)

○ 정보기술인력은 빠른 주기로 발전하는 기술에 대한 지속적인 학습이 필요하고, 다른 전통적인 작업(인사, 마케팅 등)과 달리 실시간성으로 업무를 처리해야 한다는 특성이 있어 (Chang et al, 2012<sup>6)</sup>), 전문성 개발에 관심이 높음

□ 기관의 정보보호 지식과 기술을 갖춘 전문인력에 대한 수요도 꾸준하고, 정보보호 전문인력의 자기개발에 대한 의지도 높으며, 지능정보기술의 발전으로 정보보호의 중요성도 커지고 있지만, 기업은 정보보호 전문인력 확보 및 유지에 많은 어려움을 겪고 있음

○ 보안사고가 발생했을 때 책임소재는 기업(정보보호 담당자)이 입증해야 하며, CISO(정보보호 최고책임자)의 권한은 확대되고 있지만, 보안사고 발생 시 책임이 막중 <그림 1-1>



<그림 1-1> 정보보호 담당자가 업무 변경을 희망하는 이유

※출처 : <https://www.datanet.co.kr/news/articleView.html?idxno=179877>

5) Spence, M., (1973), "Job market signaling," The Quarterly Journal of Economics, 87(3), 355-374.  
 Spence, M., (1976), "Product differentiation and welfare," The American Economic Review, 66(2), 407-414.  
 Connelly, B. L., S. T. Certo, R. D. Ireland, and C. R. Reutzel, (2011), "Signaling theory: A review and assessment," Journal of Management, 37(1), 39-67.  
 6) Chang, C. L. H., Jiang, J. J., Klein, G. and Chen, H. G. (2012), "Career anchors and disturbances in job turnover decisions-A case study of IT professionals in Taiwan," Information & Management, 49(6), 309-319.



- [기본소양 확대] 학생 다중문해력과 성인 기초 디지털 문해력 향상을 위해 디지털배움터 등의 설치를 통해 실생활 중심 체험형 교육(스마트기기 활용, 교통·금융·정부24 등), 디지털 소양 교육(기초코딩, AI, 정보보안 등) 실시
  - 사이버보안(정보보호, 정보보안 포함)은 디지털 인재가 익혀야 하는 기술요소의 하나로서 <그림 1-2>, 전문인력부터 기초인력을 대상으로 하는 디지털 교육의 하나의 학습 영역으로 포함하되, 훈련 및 교육 효과를 입증할 수 있는 자격제도가 이의 실행을 도울 수 있을 것
- 사이버보안 분야에 있어, 최정예 사이버인력 양성으로 안전한 디지털 강국 구현을 목표로 ‘사이버 10만 인재 양성 방안’ 발표<sup>8)</sup>
- ‘사이버 인력’을 정보자산을 보호하기 위한 보안 제품·서비스 개발, 보안 정책수립·관리, 사고 대응 등 사이버 공격에 대응하는 활동을 하는 인력으로 정의
  - 사이버 역량은 사이버보안 제품·서비스를 신속하게 개발하고 잘 활용하는 것이 중요하며 이는 보안인력의 역량이 좌우한다고 보고, 산업성장 등을 감안하여 사이버 인력은 12.4만 명(‘21년)에서 16.3만 명(‘26년)으로 확대되어 약 4만 명의 신규 인력 수요가 발생할 것으로 전망
  - 향후 5년(‘22년-’26년) 간 산업 수요에 대응하는 신규 인력공급(4만 명), 재직자 역량 강화 교육(6만 명) 등 10만 명 양성 추진
- 정보보호 분야의 지식 및 기술을 갖춘 전문인력에 대한 수요는 앞으로도 계속 증가할 것. 다만, 정보보호 지식 및 기술의 범주가 매우 광범위해질 것이며, 이의 전문성의 정도를 평가하고 인정해 줄 수 있는 수단이 필요
- CISO(정보보호최고책임자)/CPO(개인정보 보호책임자)로서 성장할 정도의 전문적인 지식 및 기술을 갖춘 인력도 필요하지만, 정보보호의 전산업·전사회 내재화로 인해 기초 수준의 인력도 광범위하게 필요
  - 따라서, 지능정보사회로 진입하고 있는 현시점에서 정보보호 전문성을 평가하고 증명할 수 있는 체계적이고 전문성 있는 자격제도의 마련이 필요

8) 과학기술정보통신부 (2022.7.13.), ‘사이버 10만 인재 양성 방안’ 발표 : 최정예 사이버인력 양성으로 안전한 디지털 강국 구현.

- 국외는 자격이 현장의 직무와 보다 일치되도록 일 중심의 역량(competency) 기반 자격을 설계하고 이를 기반으로 자격검정 시행<sup>9)</sup>
  - (독일) 초기 입직자가 직업세계에서 예상하지 못한 문제가 발생할 때 해결할 수 있는 역량을 갖추어 노동시장으로 진입하도록 역량 기반 출제기준을 통해 자격 검증 시행
  - (영국·호주) 영국은 국가직업표준(NOS), 호주는 훈련패키지(TP)를 개발하고, 이를 기반으로 자격을 관리·운영
  
- 국외는 정보보호 전문자격과 관련하여 국제적인 네트워크를 보유한 민간기관이 강하게 market-driven하며 브랜드화하여 확실한 시장수요를 이끌며 성장하고 있으며, 기존 자격제도의 탄탄한 기반 위에 미래 지능정보기술(빅데이터, 클라우드, 인공지능)을 결합하며 확장 중
  - 국제적으로 정보보안 분야 전문 자격제도로 인정받는 CISA(Certified Information Systems Auditor), CISSP(Certified Information System Security Professional)를 운영하는 ISACA와 ISC2는 최근 IT 기술의 고도화로 클라우드, 인공지능의 활용 등으로 정보보안 이슈가 확대되고 있다는 점을 반영하여 정보보안 부문 자격증 역시 변화를 시도 중인 것으로 파악됨
  - ISC2의 CISSP와 ISACA의 CISM 두 자격증은 모두 “관리적” 스킬을 평가하며, 벤더 독립적. 정보보안 관리 분야에서의 5년의 경험이 있어야 자격증을 취득할 수 있으며 매년 유지보수 교육을 의무 이수하여야 함
  - ISC2는 공교육에 정보보안 과정을 넣어 어렸을 때부터 보안에 대한 인지도를 높여줘야 전문가로 성장할 가능성도 높일 수 있다고 보고, Cyber Literacy 향상에 주력
    - 문제해결능력, 팀워크능력, 소통능력과 같은 소프트 스킬을 갖춘 사람을 인증하고 나아가 이 인력이 기술자격까지 갖추게 하는 것을 목표로 함 (Certified in Cybersecurity, CC)

9) 관계부처 합동 (2022.2), 제4차 자격관리·운영 기본계획(안)(2022-2026).

□ 반면, 국내는 국가자격 이외에는 시장성이 없는 상황

○ 국내 정보보호 시장(산업)이 영세하여 전문성 확보를 위한 별도의 노력이 필요한 직무임에도 불구하고 정보보호 직업만의 인센티브가 없기에 그만큼 관련 자격제도를 준비할 수요도 없는 것으로 보임

○ 국내 정보보호 분야 국가자격은 정보보안(산업)기사, 디지털포렌식전문가(2급, 부분), 산업보안관리사이며, 비교적 활성화된 민간자격(전년도 응시생 수가 있는 경우; 민간자격정보서비스<sup>10)</sup> 검색 결과)은 개인정보관리사(CPPG), 해킹보안전문가, 정보보안관제사 등이 있음

- ▶ **경제·사회 분야의 디지털 전환과 사이버보안 역량에 적합한 자격 신설 필요**
  - 디지털 트랜스포메이션의 성공을 위한 사이버보안 역량이 요구되며, 숙련된 사이버보안 인력 검증 및 사이버보안 인식을 위한 자격(2종) 신설 필요
- ▶ **정보보호 인력양성 지원·확대 및 잠재수요의 선제적 대응 필요**
  - 정보보호 인력 10만 양성 지원 및 사이버 위협에 즉시 대응 가능한 보안 분야 기획·위험평가 수행 전문가 자격이 요구되며, 해당 분야 잠재수요 대응 및 진입을 위한 보안 지식·역량 검증 수단이 필요

□ 민간자격제도는 국가자격 외의 분야에서 공인받지 못하는 개인의 지식과 기술 등을 객관적으로 평가하여 자격을 부여하여 국민의 평생직업능력개발을 장려하기 위하여 도입됨<sup>11)</sup>

○ 민간자격을 통해 자격의 취득을 위하여 교육 또는 학습에 참여가 늘어날 수 있으며, 이는 국가적으로 평생교육을 확대할 기회로 활용할 수 있음<sup>12)</sup>

□ 본 연구를 통해, 국가 디지털 인재 양성 전략의 실행을 뒷받침할 사이버보안(정보보호, 정보보안) 분야의 전문인력 및 기초인력의 실질적인 수준을 검정할 수 있는 민간자격을 도출하고, 운영방안을 수립하고자 함

10) <https://www.pqi.or.kr/indexMain.do> (민간자격정보서비스)

11) 김덕기, 김상진, 박종성 (2013.10), 민간자격제도 질 관리 방안, 한국직업능력연구원.

12) 조인식 (2021.12), 민간자격제도의 현황과 개선과제, NARS현안분석, 국회입법조사처, 제235호.

## 제 2 절 연구의 방법

- 정보보호 분야 신규 민간자격 신설 필요성 도출과 공인민간자격 등록방안 마련을 목표로 <Desk Research> 수행
  - 국내 정보보호 분야 국가 및 민간 전문 자격제도 운영 현황
  - 국외 정보보호 분야 전문 자격제도 운영 현황
  - 정보보호 산업 및 직업 트렌드 현황
  
- 민간자격 2종에 대한 문제 출제 기준 검토와 출제문제 검증을 위한 <전문가 자문> 실시
  
- 민간자격 2종의 실질적인 운영이 이루어질 수 있도록 산학연관 각계의 의견을 수렴할 수 있는 <공청회> 개최

### 제 3 절 추진계획 대비 실적 진도

- 공인 민간자격으로 등록할 정보보호 분야 민간자격 발굴 2건
- 자격 운영 및 등록방안(민간 자격의 관리운영규정) 작성 및 문제개발/검수
- 공청회 개최(11/16)

<표 1-1> 연구의 추진일정

연구 내용	가중치 (%)	추진 일정 (5개월)						참여인력 (M.Y)	활동 책임자
		7월20일 개시	8월	9월	10월	11월	12월20일 종료		
킵오프	-	▶						0.41	김태성
자격 발굴	15%		▶▶▶	▶▶▶					
자격 운영 및 등록방안 마련	30%			▶▶▶	▶▶▶				
문제개발	30%			▶▶▶	▶▶▶	▶▶▶			
활성화 방안 도출	20%					▶▶▶	▶▶		
공청회 개최	5%						▶▶		
주요 Mile-Stone 완성점에서의 연구결과		자격운영방안 수립		자격 등록방안 마련, 문제 개발		자격 활성화 방안 도출, 공청회 개최(11/16)			
연구진도 (%)		30%		80%		100%			
예산집행계획 (천원)		7,115		32,055		20,830			

## 제 2 장 공인민간자격 발굴 및 운영 방안

### 제 1 절 국내외 정보보호 관련 자격제도 현황

#### 1. 국내 정보보호 관련 국가공인 자격제도

- 2022년 말 기준 국내 국가기술자격은 총 544종 (2022년 시행 종목 기준)
  - 국가기술자격이란 「자격기본법」에 따른 국가자격 중 산업과 관련이 있는 기술·기능 및 서비스 분야의 자격으로, 국가기술자격법 시행규칙 [별표 2]에 규정된 544종목
- 2022년 국가기술자격 필기시험 응시자는 총 209만 4,718명으로, 전년 대비 15.9%(394,618명) 감소
  - 자격 취득자는 73만 8,935명으로 전년 대비 12%(100,827명) 감소, 자격 취득률은 35.3%로 전년 대비 1.5%p 상승

<표 2-1> 2022년 운영기관별 국가기술자격 시행 현황

연번	기관명	운영종목 수	필기시험 응시자	취득자
총 계		544종목	2,094,718명	738,935명
1	한국산업인력공단	493종목	1,619,461명	598,227명
2	한국방송통신전파진흥원	18종목	18,675명	4,815명
3	대한상공회의소	15종목	443,653명	131,744명
4	한국광해광업공단	7종목	317명	90명
5	한국원자력안전기술원	3종목	253명	51명
6	한국콘텐츠진흥원	3종목	424명	192명
7	영화진흥위원회	2종목	113명	54명
8	한국디자인진흥원	1종목	622명	228명
9	한국데이터산업진흥원	1종목	11,200명	3,534명
10	한국산업안전보건공단	1종목	2022년 미시행	

출처 : 고용노동부, 한국산업인력공단, 2022 국가기술자격통계연보, 2023.6.

<표 2-2> 국가기술자격 시행기관 현황 : 2022년 말 기준

기관명	종목수	종목명	수탁연도
총계	544		
한국산업인력공단	493	※국가기술자격종목 중 다른 검정기관에서 시행되는 종목을 제외한 종목	1982년
대한상공회의소	15	전자상거래관리사1/2급, 전산회계운용사 1/2/3급, 워드프로세서, 한글속기1/2/3급, 비서1/2/3급, 컴퓨터활용능력1/2급, 전자상거래운용사	1984년
한국원자력안전기술원	3	방사선관리기술사, 원자력발전기술사, 원자력기사	2008년
영화진흥위원회	2	영상산업기사, 영상기능사	2009년
한국방송통신전파진흥원	9	무선설비기사, 무선설비산업기사, 무선설비기능사, 방송통신기사, 방송통신산업기사, 방송통신기능사, 전파전자통신기사, 전파전자통신산업기사, 전파전자통신기능사	2010년
	7	정보통신기술사, 통신설비기능장, 정보통신기사, 정보통신산업기사, 통신선로산업기사, 통신선로기능사, 통신기기기능사	2012년
	2	정보보안기사, 정보보안산업기사 [*한국인터넷진흥원에서 13년부터 21년까지 시행]	2022년
한국콘텐츠진흥원	3	게임그래픽전문가, 게임기획전문가, 게임프로그래밍전문가	2010년
한국광해광업공단	2	광해방지기술사, 광해방지기사	2010년
	4	광산보안기사, 광산보안산업기사, 광산보안기능사, 시추기능사	2012년
	1	자원관리기술사	2014년
한국디자인진흥원	1	서비스·경험디자인기사	2020년
한국데이터산업진흥원	1	빅데이터분석기사	2020년
한국산업안전보건공단	1	타워크레인설치·해체기능사	2022년

국방부에서 시행하는 69종목은 한국산업인력공단(64종목), 한국방송통신전파진흥원(5종목) 시행종목과 중복 출처 : 고용노동부, 한국산업인력공단, 2023 국가기술자격통계연보, 2023.6.

- <정보기술> 부분 국가자격제도(국가기술자격)로는 빅데이터분석기사, 전자계산기조직응용기사, 정보보안기사, 정보처리기사 등의 기사와 사무자동화산업기사, 정보보안산업기사, 정보처리 산업기사 등 산업기사가 있음 <표 2-3 참조>
- 정보처리기사는 2020년에 개정을 통해 정보보안을 검정항목에 포함하기 시작

<표 2-3> 국가기술자격의 직무분야 및 국가기술자격의 종목 (정보기술 부문)

직무 분야 (26)	중직무 분야 (61)	기술·기능 분야 (506)					서비스 분야 (33)			
		기술사	기능장	기사	산업 기사	기능사	1급	2급	3급	단일 등급
총합		84개	29개	117개	119개	157개	10개	10개	3개	10개
21 정보 통신 (3개 중직무/ 31개)	211 정보 기술 (15개)									게임 그래픽 전문가
										게임기획 전문가
										게임 프로그래밍 전문가
										멀티 미디어 콘텐츠 제작 전문가
					빅데이터 분석					
						사무 자동화				
					전자 계산기 조직응용					
		정보관리								
							정보기기 운용			
					정보처리	정보처리	정보처리			
		컴퓨터 시스템 응용								
			정보보안	정보보안						

출처 : 국가기술자격법 시행규칙 별표2 (개정 2022.10.27.)

<표 2-4> 국가기술자격의 응시자 및 합격률 추이 (정보기술 부문)

(단위 : 명)

연도	시험 현황								자 격 취득자 현 황
	필기시험				실기시험				
	접수	응시	합격	합격률 (%)	접수	응시	합격	합격률 (%)	
< 정보보안기사 >									
소계	124,107	83,325	24,679	29.6	53,930	40,309	4,200	10.4	4,200
75~17	61,411	41,917	12,498	29.8	25,005	18,864	1,950	10.3	1,950
18	11,973	8,443	2,648	31.4	6,229	4,650	805	17.3	805
19	12,918	8,493	2,811	33.1	5,756	4,336	461	10.6	461
20	13,567	8,565	2,086	24.4	5,836	4,372	348	8.0	348
21	12,131	8,157	2,427	29.8	5,391	3,956	76	1.9	76
22	12,107	7,750	2,209	28.5	5,713	4,131	560	13.6	560
< 정보보안산업기사 >									
소계	26,495	18,622	7,919	42.5	12,235	9,324	2,533	27.2	2,533
75~17	13,398	9,648	4,130	42.8	5,717	4,410	1,235	28.0	1,235
18	2,393	1,748	922	52.7	1,614	1,225	288	23.5	288
19	2,495	1,738	656	37.7	1,257	982	254	25.9	254
20	2,979	1,897	873	46.0	1,193	886	332	37.5	332
21	2,540	1,812	779	43.0	1,225	923	294	31.9	294
22	2,690	1,779	559	31.4	1,229	898	130	14.5	130
< 빅데이터분석기사 >									
소계	41,390	26,120	12,670	48.5	14,085	10,997	6,357	57.8	6,357
21	22,370	14,920	6,520	43.7	5,534	4,683	2,823	60.3	2,823
22	19,020	11,200	6,150	54.9	8,551	6,314	3,534	56.0	3,534
< 정보처리기사 >									
소계	2,622,537	1,877,349	913,672	48.7	1,571,703	1,281,316	656,025	51.2	659,326
75~17	2,285,081	1,636,450	775,063	47.4	1,278,660	1,056,743	582,028	55.1	585,329
18	65,618	44,665	22,976	51.4	42,647	33,101	16,727	50.5	16,727
19	74,027	52,845	30,740	58.2	55,349	43,763	22,495	51.4	22,495
20	55,784	43,279	24,820	57.3	54,225	41,457	7,341	17.7	7,341
21	71,333	51,640	32,865	63.6	68,837	52,945	16,323	30.8	16,323
22	70,694	48,470	27,208	56.1	71,955	53,307	11,111	20.8	11,111

출처 : 국가기술자격 통계연보 (<https://www.q-net.or.kr/crf012.do?id=crf01209&gSite=Q&gld=>)  
(2023.08.19. last visited)

## (1) 정보보안기사

○ 시행처 : 한국방송통신전파진흥원

○ 정보보안기사 직무

- 시스템 및 솔루션 개발, 운영 및 관리, 컨설팅 등의 전문 이론과 실무능력을 기반으로 IT 기반시설 및 정보에 대한 체계적인 보안업무 수행

○ 응시자격 및 경력인정 기준

- 「국가기술자격법 시행령」 제12조의2(국가기술자격의 등급과 응시자격)
- 「국가기술자격법 시행규칙」 제10조의2(응시자격) 별표 11의 2에 근거하여 모든 직무분야에서 응시 가능

○ 세부응시자격

- 산업기사 등급 이상의 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 1년 이상 실무에 종사한 사람
  - 기능사 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 3년 이상 실무에 종사한 사람
  - 응시하려는 종목이 속하는 동일 및 유사 직무분야의 다른 종목의 기사 등급 이상의 자격을 취득한 사람 직무분야별 학과
  - 관련학과의 대학졸업자 등 또는 그 졸업예정자
  - 3년제 전문대학 관련학과 졸업자 등으로서 졸업 후 응시하려는 종목이 속하는 동일 및 유사 직무 분야에서 1년 이상 실무에 종사한 사람
  - 2년제 전문대학 관련학과 졸업자 등으로서 졸업 후 응시하려는 종목이 속하는 동일 및 유사 직무 분야에서 2년 이상 실무에 종사한 사람
  - 동일 및 유사 직무분야의 기사 수준 기술훈련과정 이수자 또는 그 이수예정자
  - 동일 및 유사 직무분야의 산업기사 수준 기술훈련과정 이수자로서 이수 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 2년 이상 실무에 종사한 사람
  - 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 4년 이상 실무에 종사한 사람
  - 외국에서 동일한 종목에 해당하는 자격을 취득한 사람
- ※ 정보보안 분야는 학과와 직무분야 구분 없음(모든 학과, 모든 직무분야 응시 가능)

○ 시험과목13)

<표 2-5> 정보보안기사 시험과목

과목명	주요항목	세부항목	
필 기	시스템 보안 (문제 수 20)	정보시스템의 범위 및 이해	①단말 및 서버 시스템 ②운영체제 ③시스템 정보
		시스템 보안위협 및 공격기법	①시스템 보안위협 ②시스템 공격기법
		시스템 보안위협 및 공격에 대한 예방과 대응	①시스템보안 대응기술 ②시스템 분석 도구 ③시스템 보안 솔루션
	네트워크 보안 (문제 수 20)	네트워크 일반	①네트워크 개념 이해 ②네트워크의 활용
		네트워크 기반 공격기술의 이해 및 대응	①서비스 거부(DoS), 분산 서비스 거부(DDoS) 공격 ②스캐닝 ③스푸핑 공격 ④스니핑 공격 ⑤원격접속 공격
		네트워크 보안 기술	①보안 프로토콜 이해 ②네트워크 보안기술 및 응용
	어플리케이션 보안 (문제 수 20)	인터넷 응용 보안	①FTP 보안 ②메일 보안 ③Web/App 보안 ④DNS 보안 ⑤DB 보안
		전자상거래 보안	①전자상거래 보안 기술
		어플리케이션 보안 취약점	①어플리케이션 보안취약점 대응 ②어플리케이션 개발 보안
	정보보안 일반 (문제 수 20)	보안요소 기술	①인증 ②접근통제 ③키 분배 프로토콜 ④디지털서명
		암호학	①암호 알고리즘 ②해시함수
	정보보안 관리 및 법규 (문제 수 20)	정보보호 관리	①정보보호 관리 이해 ②정보보호 위험평가 ③정보보호 대책 구현 및 사고대응 ④정보보호 인증제도 이해
정보보호 관련 윤리 및 법규		①정보보안 윤리 ②정보보호 관련 법제 ③개인정보보호 관련 법제	
실 기	정보보안 실무	시스템 및 네트워크 보안 특성 파악	①운영체제별 보안특성 파악하기 ②프로토콜별 보안특성 파악하기 ③서비스별 보안특성 파악하기 ④보안장비 및 네트워크 장비별 보안특성 파악하기
		취약점 점검 치 보완	①운영체제 보안설정 점검과 보완하기 ②서비스 보안설정 점검과 보완하기 ③네트워크 및 보안장비 설정 점검과 보완하기 ④취약점 점검이력과 보완내용 관리하기
		보안관제 및 대응	①정보수집 및 모니터링 ②로그분석 및 대응
		위험분석 및 정보보호 대책 수립	①IT 자산 위험 분석하기 ②조직의 정보자산 위험 및 취약점 분석 정리하기 ③위험평가하기 ④정보보호대책 선정 및 이행계획 수립하기

13) [https://www.cq.or.kr/qh\\_quagm01\\_020.do](https://www.cq.or.kr/qh_quagm01_020.do) (2023.08.19. last visited)

○ 검정방법

- 필기 : 100점을 만점으로 하여 과목당 40점 이상, 전과목 평균 60점 이상  
[객관식 4지선다형. 시험시간 2시간 30분]
- 실기 : 100점을 만점으로 하여 60점 이상 필답형 [3시간]

○ 응시수수료 : 필기 18,800원, 실기 21,900원

○ 사후관리 : 갱신없음

○ 자격증 혜택 : 공무원, 장교, 공기업, 민간기업, 학점인정 등 혜택 제공

## (2) 빅데이터분석기사<sup>14)</sup>

○ 시행처 : 한국데이터산업진흥원

○ 빅데이터분석기사 정의

- 빅데이터 이해를 기반으로 빅데이터 분석 기획, 빅데이터 수집·저장·처리, 빅데이터 분석 및 시각화를 수행하는 실무자를 말한다.

○ 시험과목

- 필기 : 빅데이터 분석 기획, 빅데이터 탐색, 빅데이터 모델링, 빅데이터 결과해석
- 실기 : 빅데이터 분석 실무

<표 2-6> 빅데이터분석기사 출제기준(필기)

직무분야	정보통신	중직무분야	정보기술	자격종목	빅데이터 분석기사
직무내용	대용량의 데이터 집합으로부터 유용한 정보를 찾고 결과를 예측하기 위해 목적에 따라 분석기술과 방법론을 기반으로 정형/비정형 대용량 데이터를 구축, 탐색, 분석하고 시각화를 수행하는 업무를 수행한다.				
필기검정방법	객관식	문제수	80	시험시간	120분

<표 2-7> 빅데이터분석기사 과목별 주요 항목(필기)

필기과목명	문제수	주요항목
빅데이터 분석기획	20	빅데이터의 이해 데이터 분석 계획 데이터 수집 및 저장 계획
빅데이터 탐색	20	데이터 전처리 데이터 탐색 통계기법 이해
빅데이터 모델링	20	분석모형 설계 분석기법 적용
빅데이터 결과 해석	20	분석모형 평가 및 개선 분석결과 해석 및 활용

14) [https://www.dataq.or.kr/www/sub/a\\_07.do](https://www.dataq.or.kr/www/sub/a_07.do) (2023.08.19. last visited)

<표 2-8> 빅데이터분석기사 시험과목(필기)

필기과목명	주요항목	세부항목	세세항목
빅데이터 분석 기획	빅데이터의 이해	빅데이터 개요 및 활용	①빅데이터의 특징 ②빅데이터의 가치 ③데이터 산업의 이해 ④빅데이터 조직 및 인력
		빅데이터 기술 및 제도	①빅데이터 플랫폼 ②빅데이터와 인공지능 ③개인정보 법·제도 ④개인정보 활용
	데이터분석 계획	분석방안수립	①분석 로드맵 설정 ②분석 문제 정의 ③데이터 분석 방안
		분석 작업 계획	①데이터 확보 계획 ②분석 절차 및 작업 계획
	데이터 수집 및 저장 계획	데이터 수집 및 전환	①데이터 수집 ②데이터 유형 및 속성 파악 ③데이터 변환 ④데이터 비식별화 ⑤데이터 품질 검증
데이터 적재 및 저장		①데이터 적재 ②데이터 저장	
빅데이터 탐색	데이터 전처리	데이터 정제	①데이터 정제 ②데이터 결측값 처리 ③데이터 이상값 처리
		분석 변수 처리	①변수 선택 ②차원축소 ③파생변수 생성 ④변수 변환 ⑤불균형 데이터 처리
	데이터 탐색	데이터 탐색 기초	①데이터 탐색 개요 ②상관관계 분석 ③기초통계량 추출 및 이해 ④시각적 데이터 탐색
		고급 데이터 탐색	①시공간 데이터 탐색 ②다변량 데이터 탐색 ③비정형 데이터 탐색
	통계기법 이해	기술통계	①데이터요약 ②표본추출 ③확률분포 ④표본분포
추론통계		①점추정 ②구간추정 ③가설검정	
빅데이터 모델링	분석모형 설계	분석 절차 수립	①분석모형 선정 ②분석모형 정의 ③분석모형 구축 절차
		분석 환경 구축	①분석 도구 선정 ②데이터 분할
	분석기법 적용	분석기법	①회귀분석 ②로지스틱 회귀분석 ③의사결정나무 ④인공신경망 ⑤서포트벡터머신 ⑥연관성분석 ⑦군집분석
		고급 분석기법	①범주형 자료 분석 ②다변량 분석 ③시계열 분석 ④베이지안 기법 ⑤딥러닝 분석 ⑥비정형 데이터 분석 ⑦양상블 분석 ⑧비모수 통계
빅데이터 결과해석	분석모형 평가 및 개선	분석모형 평가	①평가 지표 ②분석모형 진단 ③교차 검증 ④모수 유의성 검정 ⑤적합도 검정
		분석모형 개선	①과대적합 방지 ②매개변수 최적화 ③분석모형 융합 ④최종모형 선정
	분석결과 해석 및 활용	분석결과 해석	①분석모형 해석 ②비즈니스 기여도 평가
		분석결과 시각화	①시공간 시각화 ②관계 시각화 ③비교 시각화 ④인포그래픽
		분석결과 활용	①분석모형 전개 ②분석결과 활용 시나리오 개발 ③분석모형 모니터링 ④분석모형 리모델링

출처 : [https://www.dataq.or.kr/www/sub/a\\_07.do](https://www.dataq.or.kr/www/sub/a_07.do) (2023.08.19. last visited)

<표 2-9> 빅데이터분석기사 출제기준(실기)

직무분야	정보통신	중직무분야	정보기술	자격종목	빅데이터 분석기사
직무내용	대용량의 데이터 집합으로부터 유용한 정보를 찾고 결과를 예측하기 위해 목적에 따라 분석기술과 방법론을 기반으로 정형/비정형 대용량 데이터를 구축, 탐색, 분석하고 시각화를 수행하는 업무를 수행한다.				
실기검정방법	통합형(필답형, 작업형)		시험시간	180분	

※ 필기시험 면제기간은 필기합격자 발표일로부터 2년 (다만, 발표일부터 2년동안 검정이 2회 미만으로 시행된 경우에는 그 다음 회차 필기시험 1회를 면제)

<표 2-10> 빅데이터분석기사 과목별 주요 항목(실기)

실기과목명	주요항목	
빅데이터 분석실무	데이터 수집 작업	데이터 모형 구축 작업
	데이터 전처리 작업	데이터 모형 평가 작업

○ 응시자격 : 다음 중 하나에 해당하는 사람

1. 대학졸업자 등 또는 졸업예정자 (전공 무관)
2. 3년제 전문대학 졸업자 등으로서 졸업 후 1년 이상 직장경력이 있는 사람 (전공, 직무분야 무관)
3. 2년제 전문대학 졸업자 등으로서 졸업 후 2년 이상 직장경력이 있는 사람 (전공, 직무분야 무관)
4. 기사 등급 이상의 자격을 취득한 사람 (종목 무관)
5. 기사 수준 기술훈련과정 이수자 또는 그 이수예정자 (종목 무관)
6. 산업기사 등급 이상의 자격을 취득한 후 1년 이상 직장경력이 있는 사람 (종목, 직무분야 무관)
7. 산업기사 수준 기술훈련과정 이수자로서 이수 후 2년 이상 직장경력이 있는 사람 (종목, 직무분야 무관)
8. 기능사 등급 이상의 자격을 취득한 후 3년 이상 직장경력이 있는 사람 (종목, 직무분야 무관)
9. 4년 이상 직장경력이 있는 사람 (직무분야 무관)

※ 졸업증명서 및 경력증명서 제출 필요

○ 합격기준

- 필기 : 100점을 만점으로 하여 과목당 40점 이상, 전과목 평균 60점 이상
- 실기 : 100점을 만점으로 하여 60점 이상

○ 응시수수료 : 필기 17,800원, 실기 : 40,800원

### (3) 정보처리기사<sup>15)</sup>

- 시행기관 : 한국산업인력공단
- 관련학과 : 모든 학과 응시 가능
- 시험과목
  - 국가기술자격의 현장성과 활용성 제고를 위해 국가직무능력표준(NCS)를 기반으로 자격의 내용(시험과목, 출제기준 등)을 직무 중심으로 개편·시행 (2020.1.1.부터)
- 정보처리기사 직무
  - 컴퓨터를 효과적으로 활용하기 위해서 하드웨어뿐만 아니라 정교한 소프트웨어가 필요하다. 이에 따라 우수한 프로그램을 개발하여 업무의 효율성을 높이고, 궁극적으로 국가발전에 이바지하기 위해서 컴퓨터에 관한 전문적인 지식과 기술을 갖춘 사람을 양성할 목적으로 제정됨
- 검정방법
  - 필기 : 객관식 4지 택일형, 과목당 20문항(과목당 30분)
  - 실기 : 필답형(2시간30분)
- 합격기준
  - 필기 : 100점을 만점으로 하여 과목당 40점 이상, 전과목 평균 60점 이상
  - 실기 : 100점을 만점으로 하여 60점 이상
- 응시수수료 : 필기 19,400원, 실기 22,600원

---

15) <http://www.q-net.or.kr/crf005.do?id=crf00503&jmCd=1320> (2023.08.19. last visited)

<표 2-11> 정보처리기사 시험과목

필기시험		
과목명	활용 NCS 능력단위	NCS 세분류
소프트웨어 설계	요구사항 확인 화면 설계 애플리케이션 설계 인터페이스 설계	응용SW엔지니어링
소프트웨어 개발	데이터 입출력 구현 / 통합 구현 / 제품소프트웨어 패키징 / 애플리케이션테스트 관리 /인터페이스 구현	응용SW엔지니어링
데이터베이스 구축	SQL 응용 / SQL 활용 / 논리 데이터베이스 설계 / 물리 데이터베이스 설계 / 데이터 전환	DB엔지니어링
프로그래밍 언어 활용	서버프로그램 구현 / 프로그래밍 언어 활용 / 응용SW 기초기술 활용	응용SW엔지니어링
정보시스템 구축관리	소프트웨어개발 방법론 활용	응용SW엔지니어링
	IT프로젝트 정보시스템 구축관리	IT프로젝트관리
	소프트웨어 개발보안 구축 / 시스템 보안 구축	보안엔지니어링
실기시험		
과목명	활용 NCS 능력단위	NCS 세분류
정보처리 실무	요구사항 확인 / 데이터 입출력 구현 / 통합 구현 / 제품소프트웨어 패키징 / 서버프로그램 구현 / 인터페이스 구현 / 프로그래밍 언어 활용 / 응용 SW 기초 기술 활용 / 화면 설계 / 애플리케이션 테스트 관리	응용SW엔지니어링
	SQL 응용	DB엔지니어링
	소프트웨어 개발 보안 구축	보안엔지니어링

<표 2-12> 정보처리기사 시험과목(필기)

필기 과목명	문제 수	주요항목	세부항목
소프트웨어 설계 (NCS : 응용SW엔지니어링)	20	1. 요구사항 확인	1. 현행 시스템 분석 2. 요구사항 확인 3. 분석모델 확인
		2. 화면 설계	1. UI 요구사항 확인 2. UI 설계
		3. 애플리케이션 설계	1. 공통 모듈 설계 2. 객체지향 설계
		4. 인터페이스 설계	1. 인터페이스 요구사항 확인 2. 인터페이스 대상 식별 3. 인터페이스 상세 설계
소프트웨어 개발 (NCS : 응용SW엔지니어링)	20	1. 데이터 입출력 구현	1. 자료구조 2. 데이터 조작 프로시저 작성 3. 데이터 조작 프로시저 최적화
		2. 통합 구현	1. 모듈 구현 2. 통합 구현 관리
		3. 제품소프트웨어 패키징	1. 제품소프트웨어 패키징 2. 제품소프트웨어 매뉴얼 작성 3. 제품소프트웨어 버전관리
		4. 애플리케이션 테스트 관리	1. 애플리케이션 테스트케이스 설계 2. 애플리케이션 통합 테스트 3. 애플리케이션 성능 개선
		5. 인터페이스 구현	1. 인터페이스 설계 확인 2. 인터페이스 기능 구현 3. 인터페이스 구현 검증
데이터베이스 구축 (NCS : DB엔지니어링)	20	1. SQL 응용	1. 절차형 SQL 작성 2. 응용 SQL 작성
		2. SQL 활용	1. 기본 SQL 작성 2. 고급 SQL 작성
		3. 논리 데이터베이스 설계	1. 관계데이터베이스 모델 2. 데이터모델링 및 설계
		4. 물리 데이터베이스 설계	1. 물리요소 조사 분석 2. 데이터베이스 물리속성 설계 3. 물리 데이터베이스 모델링 4. 데이터베이스 반정규화 5. 물리데이터 모델 품질검토
		5. 데이터 전환	1. 데이터 전환 기술 2. 데이터 전환 수행 3. 데이터 정제
프로그래밍 언어 활용 (NCS : 응용SW엔지니어링)	20	1. 서버프로그램 구현	1. 개발환경 구축 2. 서버 프로그램 구현 3. 배치 프로그램 구현
		2. 프로그래밍 언어 활용	1. 기본문법 활용 2. 언어특성 활용 3. 라이브러리 활용
		3. 응용 SW 기초 기술 활용	1. 운영체제 기초 활용 2. 네트워크 기초 활용 3. 기본 개발환경 구축
정보시스템 구축관리 (NCS : 응용SW엔지니어링, DB엔지니어링, 보안엔지니어링)	20	1. 소프트웨어개발 방법론 활용	1. 소프트웨어개발 방법론 선정 2. 소프트웨어개발 방법론 테일러링
		2. IT프로젝트 정보시스템 구축관리	1. 네트워크 구축 관리 2. SW 구축 관리 3. HW 구축 관리 4. DB 구축 관리
		3. 소프트웨어 개발 보안 구축	1. SW개발 보안 설계 2. SW개발 보안 구현
		4. 시스템 보안 구축	1. 시스템 보안 설계 2. 시스템 보안 구현

<표 2-13> 정보처리기사 시험과목(실기)

실기 과목명	주요항목	세부항목
정보처리실무	1. 요구사항 확인	1. 현행 시스템 분석하기 2. 요구사항 확인하기 3. 분석모델 확인하기
	2. 데이터 입출력 구현	1. 논리 데이터저장소 확인하기 2. 물리 데이터저장소 설계하기 3. 데이터 조작 프로시저 작성하기 4. 데이터 조작 프로시저 최적화하기
	3. 통합 구현	1. 연계 데이터 구성하기 2. 연계 매카니즘 구성하기 3. 내외부 연계 모듈 구현하기
	4. 서버프로그램 구현	1. 개발환경 구축하기 2. 공통 모듈 구현하기 3. 서버 프로그램 구현하기 4. 배치 프로그램 구현하기
	5. 인터페이스 구현	1. 인터페이스 설계서 확인하기 2. 인터페이스 기능 구현하기 3. 인터페이스 구현 검증하기
	6. 화면 설계	1. UI 요구사항 확인하기 2. UI 설계하기
	7. 애플리케이션 테스트 관리	1. 애플리케이션 테스트케이스 설계하기 2. 애플리케이션 통합 테스트하기 3. 애플리케이션 성능 개선하기
	8. SQL 응용	1. 절차형 SQL 작성하기 2. 응용 SQL 작성하기
	9. 소프트웨어 개발 보안 구축	1. SW개발 보안 설계하기 2. SW개발 보안 구현하기
	10. 프로그래밍 언어 활용	1. 기본문법 활용하기 2. 언어특성 활용하기 3. 라이브러리 활용하기
	11. 응용 SW 기초 기술 활용	1. 운영체제 기초 활용하기 2. 데이터베이스 기초 활용하기 3. 네트워크 기초 활용하기 4. 기본 개발환경 구축
	12. 제품소프트웨어 패키징	1. 제품소프트웨어 패키징하기 2. 제품소프트웨어 매뉴얼 작성하기 3. 제품소프트웨어 버전관리하기

## 2. 국내 정보보호 관련 민간 자격제도<sup>16)</sup>

- 2023년 8월 20일자 기준, 공인민간자격 종목은 총 95개이며, 공인민간자격 관리자(기관)은 59개
  - 정보보호/보안 분야 자격은 ‘산업보안관리사’ 1건 <표 2-14>

<표 2-14> 공인 민간자격 검색 결과 (보호 or 보안)

등록번호	구분	자격명	자격관리기관	유형	지역	응시자수 (전년도, 명)	취득자수 (전년도, 명)
2008-0587	공인	산업보안관리사	(사)한국산업기술보호협회	법인	서울	-	-

※취득현황은 해당 기관에서 직접 입력한 정보이며, 데이터 유무와 실제 자격운영 여부와는 무관합니다.

- 2023년 7월 6일 기준, 중복을 제외한 등록민간자격 종목은 총 49,594개이며, 민간자격 관리자(기관)은 13,462개
  - 정보보호/보안 분야 자격은 184건 검색되었으며, 이 중 전년도 기준 응시자 수가 있는 자격은 18건<표 2-15>. 이외, 디지털포렌식전문가 자격은 민간자격정보서비스DB 상으로는 응시자 수가 0이지만, 현재 시험일정이 확인되기에 추가 조사
  - 검색 키워드 : 보호, 보안, 보안관제, 포렌식, 블록체인 (산업기밀, CCTV관제, 마이데이터 제외)

<표 2-15> 등록 민간자격 검색 결과 중 응시자수 1명 이상 자격 (보안 분야)

등록번호	구분	자격명	자격관리기관 [공동발급기관]	유형	지역	응시자수 (전년도, 명)	취득자수 (전년도, 명)
2010-0516	등록	개인정보관리사 (CPPG)	(사)한국씨피오포럼	법인	서울	2,254	589
2020-004188	등록	블록체인관리사 (CBM)	사단법인 한국블록체인산업협회 [(주)스마일스토리]	법인	서울	589	556
2008-0214	등록	인터넷보안전문가	(사)한국정보통신자 격협회	법인	서울	268	82
2015-004434	등록	개인정보취급사 (CPPF)	(사)한국씨피오포럼	법인	서울	183	158

16) <https://www.pqi.or.kr/indexMain.do> (민간자격정보서비스, 2023.08.19. last visited)

등록번호	구분	자격명	자격관리기관 [공동발급기관]	유형	지역	응시자수 (전년도, 명)	취득자수 (전년도, 명)
2008-0107	등록	해킹보안전문가	한국해킹보안협회	법인	서울	160	78
2011-0713	등록	개인정보보호사	(사)한국정보평가협회	법인	대전	119	55
2018-000478	등록	금융보안관리사	사단법인 금융보안원	법인	경기	118	90
2021-001189	등록	정보보호관리사	(주)한국교육진흥협회	법인	서울	94	29
2018-004239	등록	정보보호최고책임 관리사	주식회사 에스링크	법인	부산	30	17
2016-003176	등록	정보보안관제사	주식회사 에스링크	법인	부산	23	11
2020-001190	등록	개인정보보호교육 강사	주식회사 행복디자인교육컨설팅	법인	부산	11	7
2018-001384	등록	정보보안진단원	주식회사 에스링크	법인	부산	10	7
2016-006038	등록	개인정보보호지도사	한국교육컨설팅개발원	개인	인천	7	1
2017-003656	등록	정보보호활용능력	주식회사 에스링크	법인	부산	2	2
2019-001608	등록	산업보안안전관리사 자격증	한국보안안전관리협회	법인	충남	2	1
2021-001205	등록	OT보안관리사	주식회사 에스링크	법인	부산	2	1
2019-006445	등록	정보보호·정보보안 전문강사	주식회사 에스링크	법인	부산	1	-
2020-000584	등록	블록체인기술지도사	(주)창의개발교육원	법인	세종	1	-
2011-0185	부분 공인	디지털포렌식전문가	(사)한국포렌식학회 [한국인터넷진흥원]	법인	서울	-	-

※취득현황은 해당 기관에서 직접 입력한 정보이며, 데이터 유무와 실제 자격운영 여부와는 무관합니다.

(1) 개인정보관리사 (Certified Privacy Protection General, CPPG) / (사)한국씨피오포럼<sup>17)</sup>

○ 검정기준

- 개인정보보호 정책 및 대처 방법론에 대한 지식 및 능력을 갖춘 인력 또는 향후 기업 또는 기관의 개인정보 관리를 희망하는 자로서, 다음의 업무능력을 보유한 자 : 개인정보보호와 관련된 보안정책의 수립, 기업/기관과 개인정보보호의 이해, 개인정보 취급자 관리, 관련법규에 대한 지식 및 적용

○ 응시료 : 130,000원 [단체 15인 이상 20% 할인, 학생 50% 할인]

○ 응시자격 : 제한 없음

○ 합격기준 : 과목 당 40% 이상, 총점 60% 이상

<표 2-16> 개인정보관리사 과목별 문항 및 합격기준

검정과목 (대단원)	검정과목 (중단원)	문항 수	배점	출제형태	시험시간
개인정보보호의 이해	개인정보의 개요 개인정보보호의 중요성 기업의 사회적 책임	10	10	객관식 5지선다	120분
개인정보보호 제도	개인정보보호 관련 법률 체계 개인정보보호 원칙과 의무 정보주체의 권리 분쟁해결절차	20	20		
개인정보 라이프사이클 관리	개인정보 수집·이용 개인정보 저장·관리 개인정보 제공	25	25		
개인정보의 보호조치	개요 개인정보의 기술적·관리적 보호조치 기준	30	30		
개인정보 관리체계	개인정보 관리체계 개요 주요 개인정보 관리체계	15	15		

17) <https://cpptest.or.kr/new/privacy/cpp2.php> (한국씨피오포럼, 2023.08.19. last visited)

(2) 블록체인관리사 (CBM) / 사단법인 한국블록체인산업협회(18)19)20)

- 2019년 8월 31일 제1회 블록체인관리사 시험 시행
  - 국가직무능력표준(NCS)에서 블록체인 모듈이 완성됨에 따라 2020년부터 필기시험 과목은 NCS 블록체인 모듈과 동일하게 △블록체인 분석·설계 △블록체인 구축·운영 △블록체인 서비스 기획으로 변경하여 지금까지 NCS를 검정기준 개발 관련 자료로 활용
- 직무내용
  - 1급 : 국가 경쟁력 향상과 블록체인 전문인력 양성을 위한 다차원적인 블록체인 교육 프로그램 개발 사업의 수행과 기술 표준화 연구업무를 수행하고 블록체인 전문인력을 대상으로 교육할 수 있는 업무를 수행하는 것을 직무내용으로 한다.
  - 2급 : 블록체인과 관련 산업 현장에서 다양하게 적용되는 프로그램의 보급 및 평가 업무를 주로 수행하고 블록체인과 관련 산업 분야의 교육·사무·경영·컨설팅·홍보·마케팅·정보보호 및 프로그램 개발 등의 업무를 수행하는 것을 직무내용으로 한다.
  - 3급 : 블록체인과 관련 산업 현장에서 다양하게 적용되는 교육 프로그램의 보급 및 평가 업무를 주로 수행하고 블록체인과 관련 산업 분야의 교육·사무·홍보·마케팅·영업 등의 업무를 수행하는 것을 직무내용으로 한다.

○ 응시자격

<표 2-17> 블록체인관리사 응시자격

시험직종	응시자격			
	연령	학력	국적	기타
1급	해당 없음	해당 없음	해당 없음	블록체인관리사 2급 자격증의 유효기간 (합격 후 2년 이내)에 있는 자
2급	해당 없음	해당 없음	해당 없음	블록체인관리사 3급 자격증의 유효기간 (합격 후 2년 이내)에 있는 자
3급	해당 없음	해당 없음	해당 없음	-

18) <https://kbcia.or.kr/> (한국블록체인산업협회, 2023.08.19. last visited) - 자격 내용 없음

19) <http://wiki.hash.kr/index.php/블록체인관리사>

20) (사)한국블록체인산업협회 공고 제2021-16호 : 2022년도 블록체인관리사(CBM) 자격시험 시행계획 공고

○ 응시료

- 1급·2급·3급 필기 150,000원, 1급·2급 실기 150,000원

○ 검정과목

<표 2-18> 블록체인관리사 검정과목

시험직종	시험과목 (문항 수)	시험방법	배점	합격기준	
1급	필기	객관식 4지 택 1형	블록체인 분석·설계 (20)	100	매 과목 40점 이상, 전과목 평균 60점 이상
			블록체인 구축·운영 (20)	100	
			블록체인 서비스 기획 (20)	100	
	실기	주관식 논술 사례형	블록체인 암호학 (7)	100	
			컴퓨터 작업형	100	
2급	필기	객관식 4지 택 1형	블록체인 분석·설계 (30)	100	
			블록체인 구축·운영 (30)	100	
			블록체인 서비스 기획 (30)	100	
			블록체인 암호학 (30)	100	
	실기	컴퓨터 작업형	100		
3급	필기	객관식 4지 택 1형	블록체인 분석·설계 (40)	100	
			블록체인 구축·운영 (20)	100	
			블록체인 구축·운영 (20)	100	
			블록체인 서비스 기획 (40)	100	

(3) 인터넷보안 전문가 / (사)한국정보통신자격협회<sup>21)</sup>

- 서버를 보호하고 보안 설정, 보안분석, 해킹방지, 서버복구 등 서버에 대한 해킹에 효과적으로 대처하고 정보를 보호할 수 있는 인터넷 보안 관련 기술력에 대한 자격
  - 1급 : Linux, Windows 계열을 기반으로 한 서버에서 인터넷 보안과 관련한 보안관리, 침해 사고 대응, 해킹예방, 시스템 분석 등의 전문능력을 검정
  - 2급 : Linux, Windows 계열을 기반으로 한 서버에서 인터넷 보안과 관련한 보안관리, 침해 사고 분석 및 대처의 실무능력을 검정

<표 2-19> 인터넷보안 전문가 검정료

등급	과목	검정료	입금방법
1급	필기	43,000원	무통장입금, 신용카드, 온라인이체
	실기	100,000원	
2급	필기	43,000원	무통장입금, 신용카드, 온라인이체

<표 2-20> 인터넷보안 전문가 과목별 문항 및 합격기준

등급	검정방법	검정과목	문항 수	유형	만점	합격점수
1급	필기	정보보호 개론	60 (60분)	택일형	100점	60점 이상
		운영체제				
		네트워크				
		보안				
	실기	침해사례 분석	1~20 (120분)	작업/서술/ 선택형 등	100점	60점 이상
		침해과정 분석				
		시스템서비스 관리				
		코드분석				
2급	필기	정보보호 개론	60 (60분)	택일형	100점	60점 이상
		운영체제				
		네트워크				
		보안				
	실기	침해사례 분석	1~20 (120분)	작업/서술/ 선택형 등	100점	60점 이상
		침해과정 분석				
		시스템서비스 관리				
		코드분석				
		해결책 및 예방책				

21) <https://www.icqa.or.kr/cn/page/internet> (한국정보통신자격협회, 2023.08.19. last visited)

(4) 해킹보안전문가 (Hacking & Security Expert) / 한국해킹보안협회<sup>22)</sup>

○ 해킹보안 전문가로서 갖추어야 할 지식에 대한 검정과 실무에 적용할 수 있는 능력을 검정

○ 응시료

- 1급 : 준비 중
- 2급 : 필기 50,000원, 실기 50,000원 [정기검정]
- 3급 : 50,000원 [온라인검정]
- 주니어 : 25,000원 [온라인검정]

<표 2-21> 해킹보안 전문가 과목별 문항 및 합격 기준

등급	유형	과목별 문항	만점	합격점수
1급 (준비 중)	필기	70문항	400점	평균 60점 이상 / 과목별 40점 이상 평균 60점 이상
	실기	20문항	1000점	
2급	필기	70문항(70분)	400점	평균 60점 이상 / 과목별 40점 이상 평균 60점 이상
	실기	20문항(100분)	100점	
3급	필기	50문항(50분)	100점	평균 60점 이상
주니어	필기	40문항(50분)	100점	평균 60점 이상

○ 직무내용

- 1급 : 해킹보안에 대한 고급 지식과 실무능력을 검증하며, 정보보안 분야의 전문가임을 인증할 수 있도록 한다.
- 2급 : 해킹보안에 대한 좀 더 깊이 있는 지식을 다루며, 실무에서 필요로 하는 내용을 평가 및 인증시험에 반영하여 관련업체에 취업을 하거나 높은 수준의 보안 관련 분야에 적용할 수 있는 실력을 갖출 수 있도록 한다.
- 3급 : ICT에 관심있는 고교생 및 직장인 등 해킹과 보안에 대한 올바른 윤리관과 기본지식을 쌓을 수 있도록 하여 정보화 사회에 대비한 관련 분야의 기본실력을 갖춘 인력을 양성
- 주니어급 : 초등학교 수준을 자격급수로 해킹보안 관련 기초지식의 습득 정도를 확인한다.

22) [https://www.nahs.or.kr/license/license\\_guide.php](https://www.nahs.or.kr/license/license_guide.php) (한국해킹보안협회, 2023.08.19. last visited)

○ 응시자격

<표 2-22> 해킹보안 전문가 응시자격

자격등급	응시자격
1급	대학교 졸업자 또는 졸업예정자 2급 자격을 취득한 자
2급	3급 자격을 취득한 후 6개월 이상이 경과한 자 2년제 IT직업전문학교 관련학과 졸업자 또는 졸업예정자 4년제 대학졸업자 또는 졸업예정자 직업학교 또는 직업전문학교 컴퓨터 관련학과 졸업자 또는 졸업예정자
3급	자격제한 없음
주니어	자격제한 없음

(5) 개인정보보호사 / (사)한국정보평가협회<sup>23)</sup>

- 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 안정성 확보에 필요한 기술적·관리적·물리적 조치를 수행하는 직무
- 합격기준
  - 전 과목 평균 100점 만점에 60점 이상
  - 3과목 중 과목 획득 점수 40점 미만 과락으로 불합격
- 응시료 : 50,000원

<표 2-23> 개인정보보호사 검정내용

검정방법	검정과목 (분야, 영역)		주요 내용	문항 수
필답형 (객관식)  5지 선단형  90분	개인정보 보호 및 제도	개인정보보호 개요	- 법과 컴플라이언스의 개요 - 개인정보의 이해 - 개인정보보호법의 배경	30
		개인정보 법률 체계	- 개인정보의 주체와 객체 - 개인정보보호 관련 법률 체계 - 세이프 하버 협정과 OECD 8원칙	
		개인정보보호 제도	- 정보통신망 이용촉진 및 정보보호에 관한 법률 - 정보통신망 고시	
	개인정보 관리 및 관리체계	개인정보보호 라이프사이클	- 개인정보의 수명주기 수집 / 제공 / 위탁 / 이용 / 파기	30
		개인정보 주체 관리	- 개인정보 주체의 권리 - 개인정보 분쟁 조정 - 개인정보 단체 소송 - 법정대리인 권리 - 개인정보 처리 정지 및 정정 삭제 권한	
		개인정보보호 내부 관리 계획	- 개인정보보호책임자 역할 - 개인정보보호 교육 - 개인정보 영향평가 - 개인정보 처리업무 위탁에 따른 개인정보보호	
	개인정보 보호 대응	개인정보 처리방침	- 개인정보 취급 방침 및 수립 - 개인정보 공개 - 개인정보 이용 내역 통지 - 민감정보 및 고유식별정보처리 제한	30
		개인정보 침해대응	- 개인정보 유·누출 방지 - 개인정보 침해대응 및 재해 대응절차	
		개인정보보호 조치 기준	- 개인정보 암호화 - 안전조치 의무 - 기술보안, 물리보안, 관리보안 - 영상정보처리기기 조치	

23) <https://www.kie.or.kr/kiehomepage/fc/licenceISMG1?licence=> (한국정보평가협회, 2023.08.19. last visited)

(6) 금융보안관리사(Certified Financial Security Expert, CFSE) / 사단법인금융보안원<sup>24)</sup>

○ 응시조건

- IT 및 정보보호 경력 3년 이상인 사원기관 재직자 중 전체 교육과정 80% 이상 수료자 (교육비 무료)

<표 2-24> 금융보안관리사 교육과정

구분	과목명	시간
1과목	금융비즈니스	7시간 내외
2과목	금융보안관리체계	17시간 내외
3과목	금융IT보안	25시간 내외
4과목	전자금융보안	26시간 내외

- 검정방법 : 4지선다 객관식 100문항, 총 4개 과목 100점 만점 기준 총점 60점 이상

<표 2-25> 금융보안관리사 자격시험

시험과목	문항수	배점	합격기준
금융 비즈니스	10문항	10점	4점
금융보안 관리체계	25문항	25점	10점
금융IT보안	30문항	30점	12점
전자금융 보안	35문항	35점	14점
총 4개 과목	100문항	100점	총점 60점 이상

- 금융보안관리사 자격 취득자의 전문성 유지 및 직무능력 향상을 위해 자격유지교육 (Continuing Professional Education)을 자격증 갱신요건으로 규정
  - 자격증 유효기간 3년 이내 42시간(매년 최소 10시간 이상) CPE 인정 활동을 수행한 경우 자격증 갱신

24) [https://edu.fsec.or.kr/page/client\\_guide\\_application\\_qualify](https://edu.fsec.or.kr/page/client_guide_application_qualify) (금융보안교육센터, 2023.08.19. last visited)

(7) 정보보안관제사 / 주식회사 에스링크<sup>25)</sup>

○ 정보보안관제사란

- 정보시스템의 서버(시스템), 네트워크 장비 및 정보보안장비에 대한 전문지식과 운용기술을 갖추고, 이와 더불어 실시간 정보보안관제 기술과 능력, 보안정책수립과 보안대책 구현, 취약점 진단 및 침해사고 분석의 기술, 정보보호 관련 법규 준수 여부 등 다양한 보안전문 능력을 보유하고, 사이버공격에 대한 신속하고 정확한 대응 업무 수행 능력을 갖추고 있는 자

○ 시험과목

<표 2-26> 정보보안관제사 시험 과목 및 방법

구분	문항 수				문제 유형	검정 시간	합격 기준	
	1급	2급	3급					
			일반	주니어				
필기	1. 보안관제 일반	20	20	20	25	객관식 4지 택일형	<1급> 90분  <2/3급> 60분	평균 60점 이상 각 과목 40점 이상
	2. 보안관제 기술	20	20	20	25			
	3. 보안관제 운용	20	20	20	×			
	4. 취약점 진단 기술	20	20	×	×			
	5. 침해사고 분석 기술	20	×	×	×			
		100	80	60	50			
실기	정보보안관제 실무	고급형	중급형	×	×	주관식 필답형	<1급> 120분 <2급> 90분	60점 이상
시험 접수		온라인	온라인	온라인	온라인			

\* 단답형 문제 : 20문항 × 2점 = 40점

\* 서술형 문제 : 3문항 × 10점 = 30점

\* 작업형 문제 : 2문항 × 15점 = 30점

25) <http://www.wwwcap.or.kr/isc/isc42.htm> (주식회사 에스링크, 2023.08.19. last visited)

○ 응시자격

<표 2-27> 정보보안관제사 응시자격

등급	세부 응시 자격	연령/학력
1급	1. 기사 등급 이상의 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야 <1년 이상> 실무에 종사한 사람 2. 기능사 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 <3년 이상> 실무에 종사한 사람 3. 4년제 대학 관련학과 졸업자등으로서 졸업 후 응시하려는 종목이 속하는 동일 및 유사 직무 분야에서 <1년 이상> 실무에 종사한 사람 4. 3년제 전문대학 관련학과 졸업자등으로서 졸업 후 응시하려는 종목이 속하는 동일 및 유사 직무 분야에서 <2년 이상> 실무에 종사한 사람 5. 2년제 전문대학 관련학과 졸업자등으로서 졸업 후 응시하려는 종목이 속하는 동일 및 유사 직무 분야에서 <3년 이상> 실무에 종사한 사람 6. 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 <5년 이상> 실무에 종사한 사람 7. 외국에서 동일한 종목에 해당하는 자격을 취득한 사람	4년제 대학 관련학과 졸업 후 (기사 자격 후) 경력 1년 이상  <2급 취득 후> 관련 실무경력 2년 이상 응시 가능
2급	1. 기능사 등급 이상의 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에 <1년 이상> 실무에 종사한 사람 2. 응시하려는 종목이 속하는 동일 및 유사 직무분야의 다른 종목의 <산업기사 등급> 이상 자격을 취득한 사람 3. 관련학과의 2년제 또는 3년제 전문대학졸업자 등 또는 그 졸업예정자 < 관련학과 2학년 80학점이상(학점은행제 포함) 이수자부터 응시 가능 > 4. 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 <1년 이상> 실무에 종사한 사람 5. 외국에서 동일한 종목에 해당하는 자격을 취득한 사람 6. [ 3급 ] 자격취득 후 <실무경력 1년 이상> 습득한 사람	전문대학 졸업예정자 이상  (기능사 자격 후) 경력 1년 이상  <3급 취득 후> 바로 응시 가능
3급	1. 응시하려는 종목이 속하는 동일 및 유사 직무분야의 다른 종목의 <기능사 등급> 이상의 자격을 취득한 사람 2. 중등학교 졸업자 등 또는 그 졸업예정자 3. 동일 및 유사 직무분야의 기능사 수준 기술훈련과정 이수자 또는 그 이수예정자 4. 외국에서 동일한 종목에 해당하는 자격을 취득한 사람	중등학교 졸업예정자 이상 <제한없음>

○ 수수료

- 1급 : 필기 55,000원, 실기 66,000원
- 2급 : 필기 44,000원, 실기 55,000원
- 3급 : 필기 44,000원

(8) 디지털포렌식전문가 / (사)한국포렌식학회<sup>26)</sup>·한국인터넷진흥원

○ 개요

- 디지털 포렌식 분석자의 전문성을 검증하기 위하여 디지털포렌식전문가 1급 자격제도를 운영하고 있다.
- 2급 시험은 현장에서 디지털 증거의 무결성 및 원본성을 증거수집자의 능력을 검증한다면, 1급 시험은 2급 시험에서 요구되어지는 능력에 더하여 디지털 증거 분석에 수반되는 더 높은 수준의 전문성에 초점을 두어 분석자의 전문성을 검증한다.

○ 합격기준 : 각 과목 40점 이상, 평균 60점 이상

○ 응시료

- 1급 : 필기 100,000원, 실기 250,000원 (자격증 발급 10,000원)
- 2급 : 필기 60,000원, 실기 150,000원 (자격증 발급 10,000원)

○ 시험과목

<표 2-28> 디지털포렌식전문가 시험 과목 및 방법 (1급)

구분	필기	실기
필수	디스크 포렌식	
선택	네트워크 포렌식	
	데이터베이스 포렌식	
	모바일 포렌식	
	참해사고 대응 포렌식	
필수	증거법	-
유형	서술형	실습형
합격기준	각 과목 40점 이상, 평균 60점 이상	

26) <https://exam.forensickorea.org/> (한국포렌식학회, 2023.08.19. last visited)

<표 2-29> 디지털포렌식전문가 시험 과목 및 방법 (2급)

구분	필기	실기
과목	컴퓨터 구조와 디지털 저장매체	디지털 포렌식 기초실무
	파일시스템과 운영체제	
	응용프로그램과 네트워크의 이해	
	데이터베이스	
	디지털포렌식 개론 (기초실무, 법률이론)	
유형	객관식 선다형	실습형
합격기준	각 과목 40점 이상, 평균 60점 이상	

○ 응시자격 (1급)

- 디지털포렌식 전문가 2급 자격을 보유하고 2년 이상 유관경력이 있는 사람 (단, 자격 취득 후 학회 주관 보수교육을 매년 8시간 이상 이수한 사람에 한 함)
- 석사 이상의 유관학력을 취득한 후, 2년 이상의 유관경력이 있는 사람
- 변호사나 변리사, 공인회계사로서 3년 이상의 유관경력이 있는 사람
- 유관자격을 보유한 사람으로서 3년 이상의 유관경력이 있는 사람

○ 응시자격 (2급)

- 제한없음

### 3. 국외 정보보호 관련 자격제도

- 미국 정부가 NICE 이니셔티브를 통해 운영중인 [www.cyberseek.org](http://www.cyberseek.org)에서는 사이버보안 직무와 사이버보안 인력이 주로 보유하고 있는(또는 주로 요구하는) 자격제도 6개를 매칭 : Security+, CISSP, GIAC, CISA, CISM, CIPP
- CbyerGuard가 선정한 IT전문가를 위한 10대 사이버보안 자격제도<sup>27)</sup> : CEH, CRISC, CIPP/US, CISM, CISA, CISSP, CCNA, CCNP, Security+, CHFI
- coursera가 선정한 인기 있는 10대 사이버보안 자격제도(미국 내 주요 구인광고사이트에 게시된 자료 분석 결과)<sup>28)</sup> : CISSP, CISA, Security+, CEH, CISM, GSEC, SSCP, CASP, GCIH, OSCP <표 2-30>

<표 2-30> 미국 내 구인구직사이트에서의 자격증 검색 건수 (22년 12월)

Certification	LinkedIn	Indeed	Simply Hired	Total
CISSP	159,912	14,401	8,780	183,093
CISA	37,606	7,688	4,019	49,313
Security+	7,366	10,161	3,235	20,762
CEH	16,402	2,425	1,468	20,295
CISM	8,436	4,145	2,573	15,154
GSEC	4,335	3,062	2,308	9,705
SSCP	4,046	3,013	2,160	11,865
CASP	3,783	1,128	868	5,778
GCIH	3,166	2,010	1,403	6,569
OSCP	2,095	1,850	946	4,891

출처 : <https://www.bls.gov/opub/ted/2023/job-openings-increased-to-11-0-million-in-december-2022.htm>

- CybersecurityGuide가 소개하고 있는 사이버보안 분야 자격제도<sup>29)</sup> : ①CISA, ②CEH, ③CISSP, ④CISM, ⑤Security+, ⑥CASP+(Advanced Security Practitioner - CompTIA 제공), ⑦CND(Certified Network Defender - EC Council 제공), ⑧Forensic 계열, ⑨OSCP, ⑩CRISC, ⑪Pen Testing 계열, ⑫CTIA

27) <https://cybersguards.com/cyber-security-training/> (10 Hot Cybersecurity Certifications) (2023.08.19. last visited)

28) <https://www.coursera.org/articles/popular-cybersecurity-certifications> (2023.08.19. last visited)

29) <https://cybersecurityguide.org/programs/cybersecurity-certifications/> (2023.08.19. last visited)

- Forensic 계열 세부 자격증 : ㉔Certified Digital Forensics Examiner (CDFE) - Milie2제공, ㉕Computer Hacking Forensic Investigator (CHFI) - EC-Council 제공, ㉖Certified Forensic Computer Examiner (CFCE) - IACIS 제공, ㉗GIAC Certified Forensic Examiner (GCFE) - SANS 제공, ㉘GIAC Advanced Smartphone Forensics (GASF) - SANS 제공, ㉙EnCase Certified Examiner (EnCE) & ㉚EnCase Certified eDiscovery Practitioner (EnCEP) - 벤더 OpenText 제공
  - Pen Testing 계열 세부 자격증 : ㉛Certified Ethical Hacker (CEH), ㉜GIAC Penetration Tester (GPEN), ㉝Licensed Penetration Tester (LPT) Master, ㉞Offensive Security Certified Professional (OSCP))
- 2023년 INFOSEC(보안 전문 교육기관 및 자격증 운용기관)이 선정한 7대 보안 분야 자격증<sup>30)</sup>  
: CompTIA Security+ (SY0-601), EC-Council Certified Ethical Hacker (CEHv11), (ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP), ISACA Certified Information Security Manager (CISM), ISACA Certified Information Systems Auditor (CISA), (ISC)<sup>2</sup> Certified Cloud Security Professional (CCSP), GIAC Security Essentials (GSEC)
- 2023년 INDEED(구인구직사이트)가 선정한 10대 보안 분야 자격증<sup>31)</sup> : CompTIA Security+, CompTIA PenTest+, CompTIA Cybersecurity Analyst (CySA+), CompTIA Advanced Security Practitioner (CASP+), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), GIAC Security Essentials (GSEC), Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), Certified Cloud Security Professional (CCSP)
- 2023년 simplilearn가 선정한 10대 보안 분야 자격증과 동일<sup>32)</sup>

---

30) <https://resources.infosecinstitute.com/topics/professional-development/7-top-security-certifications-you-should-have/> (2023.08.19. last visited)

31) <https://resources.infosecinstitute.com/topics/professional-development/7-top-security-certifications-you-should-have/> (2023.08.19. last visited)

32) <https://www.simplilearn.com/top-10-information-security-certification-article> (2023.08.19. last visited)

<표 2-31> 국외 주요 정보보호 분야 자격제도(관리적 정보보호) 현황

구 분	내용
CISSP (Certified Information Systems Security Professional)	<ul style="list-style-type: none"> <li>▶ CISSP를 가지고 사이버보안 커리어를 시작해 나갈 수 있을 것. CISSP credential은 세계 수준의 사이버보안 프로그램을 계획, 실행, 유지할 수 있는 능력이 있음을 증명하기 때문</li> <li>▶ 2020년 7월을 기준으로 전세계 약 14만 명이 CISSP 자격증을 보유</li> <li>▶ 이는 국제 정보시스템 보안 인증 컨소시엄(ISC squared)가 제공하며 자산 보안, 엔지니어링, 접근 관리 등 핵심 공통 지식 체계(CBK) 영역을 다룸</li> <li>▶ 자격증 요건은 최소 2개의 CBK 도메인에서 최소 5년의 경력이나 2개의 CBK 도메인과 대학 학위에서 4년 경력을 포함</li> </ul>
CISA (Certified Information Systems Auditor)	<ul style="list-style-type: none"> <li>▶ 정보기술 및 정보시스템을 감사, 관장, 추적, 분석할 능력을 지닌 인력임을 국제적으로 인정받도록 해 주는 자격제도</li> <li>▶ ISACA에서 제공하는 또 다른 자격증으로 정보 감사에 중점을 두고 있으며, IT전문가의 감사 경험을 테스트하고 취약점 관리 능력을 입증</li> <li>▶ 자격요건은 사이버보안 전문가 경력 5년. 시험은 4시간이며 객관식 150문항</li> </ul>
CISM (Certified Information Security Manager)	<ul style="list-style-type: none"> <li>▶ 보안 및 위험 관리 업무에 관심 있는 IT전문가를 위한 상급 자격증</li> <li>▶ ISACA(Information Systems Audit and Control Association)에서 요구하는 자격 조건은 사이버보안 분야 경력 5년간과 보안 관리 분야 경력 3년.</li> <li>▶ 4시간에 200문제를 풀어야 함</li> </ul>
CRISC (Certified in Risk and Information Systems Control)	<ul style="list-style-type: none"> <li>▶ IT 및 기업 위험관리를 위한 훈련이 잘 되어 있음을 증명하는 자격증으로, 이 자격증을 보유한 인력들을 비즈니스 파트너가 될 수 있는 수준으로 성장할 수 있도록 도움</li> <li>▶ 중간 수준의 IT/IS 감사자, 위험 및 보안 전문가에게 적합한 자격증</li> </ul>
CIPP (Certified Information Privacy Professionals)	<ul style="list-style-type: none"> <li>▶ CIPP는 지역으로 나누어 자격증명을 부여. 아시아 CIPP/A, 캐나다 CIPP/C, 유럽 CIPP/E, 미국 민간영역 CIPP/US, 미국 정부영역 CIPP/G (아직 미 실시)</li> <li>▶ CIPP/US의 경우, 미국 내 프라이버시 법제도에 대한 이해능력 평가</li> <li>▶ ANSI/ISO 사양과 국제인증포럼(International Accreditation Forum) 표준에 따라 인정되는 업계 유일의 인증 (CIPP, ICPM, CIPT 공통)</li> </ul>
CIPT (Certified Information Privacy Technologist)	<ul style="list-style-type: none"> <li>▶ CIPT 자격증은 인력이 속한 조직의 프라이버시 체계를 보다 정교화할 수 있는 지식을 갖추고 있음을 보장: ①개발의 모든 단계에서 데이터 보호를 고려한 프라이버시 친화적 제품, 서비스, 절차 개발 ②새롭게 출현하는 기술의 혜택과 위협을 식별하고 이들이 고객 프라이버시를 존중할 수 있도록 사용하기 위한 방법 강구 ③다양한 장애물로부터 데이터 보호 ④보다 나은 프라이버시 보장을 위한 소프트웨어 및 시스템 설계</li> </ul>
CHFI (Computer Hacking Forensic Investigator)	<ul style="list-style-type: none"> <li>▶ 세계의 경찰, 정부, 민간기업 모두가 컴퓨터 조사 기술을 사용하며, 그들의 대다수가 이 자격증에 의존</li> <li>▶ 타겟 시스템의 결점과 취약성을 찾아내는 방법을 잘 이해하도록 훈련된 전문가로 인정. 고용주는 악의적인 해커에 맞먹는 수준의 기술과 툴을 보유한 인력을 고용한 것이라 할 수 있음</li> </ul>

구 분	내용
	<ul style="list-style-type: none"> <li>▶ 전자상거래 컨설턴트 위원회(EC-Council)가 제공하는 중간 수준의 자격증</li> <li>▶ 이 자격증을 획득하려면 시험을 통과해야 하며, 5일간의 교육과정 이수 후 시험을 치름</li> </ul>
CEH (Certified Ethical Hacker)	<ul style="list-style-type: none"> <li>▶ 해커로서 필요한 스킬을 보유하고 있음을 증명. 그러나 도덕적인 요소로서 법이 허용하는 범위 내에서 활동함을 보장</li> <li>▶ 세계적으로 23.7만 명이 보유하고 있으며 민간 및 공공기관에서 활동</li> <li>▶ Security Analyst, Computer Forensics Analyst, Security Specialist, Penetration Tester, Security Engineer, Security Code Auditor, Malware Analyst, Security Consultant 등에게 적합한 자격증</li> </ul>
(CompTIA) Security+	<ul style="list-style-type: none"> <li>▶ IT 전문가가 취득할만한 첫 번째 자격증이라고 할 수 있음. 이 자격증은 대부분의 보안 기능과 서비스를 위해 필요한 기본적인 지식을 테스트하며, 중간 수준의 사이버보안 직위로 나아갈 수 있는 발판이 될 것</li> <li>▶ 기업에서 종사하는 전문가들은 CompTIA의 4개 자격증을 획득할 수 있음 : CompTIA IT Fundamentals, CompTIA A+, CompTIA Network+, CompTIA Security+. Security+는 위험관리, 완화, 위협 관리의 경향에 중점을 두고 사이버보안의 기본 기술을 다룸</li> <li>▶ 자격증을 취득하려면 IT와 네트워크 보안 분야에서 최소 2년 경력이 필요. 시험은 90분이며 최대 90문항</li> <li>▶ Junior Network Administrator, Datacenter Support Technician, Network Engineer, System Administrator, NOC Technician, Telecommunications Technician, Cable Technician 등에게 적합한 자격증</li> <li>▶ 이외에도 CompTIA는 Cybersecurity Analyst (CySA+), CompTIA Advanced Security Practitioner (CASP+), CompTIA PenTest+ 등의 자격증도 운영</li> </ul>
GSEC (GIAC Security Essentials Certification)	<ul style="list-style-type: none"> <li>▶ IT시스템 및 정보보안 기술을 입증하고자 하는 IT전문가를 위한 초급 수준의 자격시험</li> <li>▶ 실제 보안 애플리케이션의 일반적인 보안 모범 사례와 방법을 다루며, 이 자격증 시험 응시자는 접근 제어, 암호 관리, 네트워크 매핑 등에 대한 기술을 습득하는 경향이 있음</li> <li>▶ GSEC는 기술 중심의 자격증으로서 방어 알고리즘과 그의 구현, 사고대응, 침투테스트, 엔드포인트 보안 등을 다룸</li> <li>▶ GSEC 시험은 5시간 동안 180문항</li> </ul>
GSE (GIAC Security Expert)	<ul style="list-style-type: none"> <li>▶ GIAC (SANS Institute)가 수여하는 가장 어려운 자격증 중 하나</li> <li>▶ 기술 전문가임을 인증하는 최상급 자격증이며, 무엇보다도 정보보안에 특화된 숙련도를 보유하고 있음을 인증</li> <li>▶ 응시자는 이미 GSEC, GCIA 및 GCIH(모두 GIAC / SANS Institute 제공)를 보유하고 있어야 하며, 이들 3개 중 2개에서 GIAC Gold 점수를 획득해야 하며, 2개의 GIAC Gold Achievement에서 임계 점수가 80점 이상이어야 함</li> <li>▶ GSE 시험은 작문, 조사, 실제 실무 작업, 단독 발표 및 팀과제(solo presentation and group work)를 23시간 동안 현장 감독 아래 수행</li> </ul>

- 국외 주요 정보보호 분야 자격제도의 응시료<sup>33)</sup> (미국 달러 기준, 2023년)
  - Certified Information Systems Security Professional (CISSP) : \$749 (≒100만 원)
  - Certified Information Systems Auditor (CISA) : 회원 \$575, 비회원 \$760 (≒102만 원)
  - Certified Information Security Manager (CISM) : 회원 \$575, 비회원 \$760 (≒102만 원)
  - Certified in Risk and Information Systems Control (CRISC) : \$760 (≒102만 원)
  - CompTIA Security+ : \$370 (≒50만 원)
  - Certified Ethical Hacker (CEH) : \$950 to \$1,199 (시험 지역에 따라 다름) (≒127만~160만)
  - GIAC Security Essentials Certification (GSEC) : \$2,499 (연습 문제 2회 포함) (≒334만 원)
  - Systems Security Certified Practitioner (SSCP) : \$249 (≒33만 원)
  - CompTIA Advanced Security Practitioner (CASP+) : \$466 (≒62만 원)
  - GIAC Certified Incident Handler (GCIH) : \$2,499 (연습 문제 2회 포함) (≒334만 원)
  - Offensive Security Certified Professional (OSCP) : From \$999 (Basic package includes Penetration Testing with Kali Linux (PWK/PEN-200) course, 30 days of lab access, and one exam attempt) (≒134만부터)
  
- ISC2(International Information System Security Certification Consortium, 1989년부터) 운영 자격증 현황은 <표 2-32>와 같음<sup>34)</sup>
  - ISC2는 사이버보안 전문가를 위한 교육 및 인증을 전문으로 하는 비영리 조직
  
- ISACA(Information Systems Audit and Control Association, 1969년부터) 운영 자격증 현황은 <표 2-33>과 같음<sup>35)</sup>
  - IT 거버넌스에 중점을 둔 국제 전문가 협회
  - 전문 자격증(ISACA CERTIFICATIONS) 5종 운영 : CISA, CISM, CRISC, CDPSE, CGEIT
  - 자격 인증(ISACA CERTIFICATES) 7종 운영 : CCAK(Certificate in Cloud Auditing Knowledge), COBIT, Cybersecurity Audit, Cybersecurity Fundamentals, Emerging Technology, IT Audit Fundamentals, IT Risk Fundamentals

33) <https://www.coursera.org/articles/popular-cybersecurity-certifications> (2023.08.19. last visited)

34) <https://www.isc2.org/certifications> (2023.08.19. last visited)

35) <https://www.isaca.org/credentialing> / <https://www.isaca.org/credentialing/certifications> (2023.08.19. last visited)

<표 2-32> ISC<sup>2</sup> 운영 자격증

\* ANAB : ANSI National Accreditation Board

<p style="text-align: center;"><b>CCSM</b> * <b>Certified in Cybersecurity</b></p> <p>Entry-Level (업무경력 필요없음) 무료 시험&amp;교육 (제한시간 내)</p> <p>[시험과목] 1. Security Principles 2. Business Continuity (BC), Disaster Recovery (DR) &amp; Incident Response Concepts 3. Access Controls Concepts 4. Network Security 5. Security Operations</p>	<p style="text-align: center;"><b>CCSP®</b> * <b>Certified Cloud Security Professional</b></p> <p>5년 이상 업무경력 필요 ANAB(ISO/IEC표준 17025) U.S.DoD 8570.1(국방부승인)</p> <p>[시험과목] 1. Cloud Concepts, Architecture and Design 2. Cloud Data Security 3. Cloud Platform &amp; Infrastructure Security 4. Cloud Application Security 5. Cloud Security Operations 6. Legal, Risk and Compliance</p>	<p style="text-align: center;"><b>CISSP®</b> * <b>Certified Information Systems Security Professional</b></p> <p>5년 이상 업무경력 필요 ANAB(ISO/IEC표준 17024) U.S.DoD 8570.1(국방부승인)</p> <p>[시험과목] 1. Security and Risk Management 2. Asset Security 3. Security Architecture and Engineering 4. Communication and Network Security 5. Identity and Access Management (IAM) 6. Security Assessment and Testing 7. Security Operations 8. Software Development Security</p>
<p style="text-align: center;"><b>CGRC<sub>SM</sub></b> * <b>Governance, Risk and Compliance Certification</b></p> <p>2년 이상 업무경력 필요 ANAB(ISO/IEC표준 17026) U.S. DoD 8570.1(국방부승인)</p> <p>[시험과목] 1. Information Security Risk Management Program 2. Scope of the Information System 3. Selection and Approval of Security and Privacy Controls 4. Implementation of Security and Privacy Controls 5. Assessment/Audit of Security and Privacy Controls 6. Authorization/Approval of Information System 7. Continuous Monitoring</p>	<p style="text-align: center;"><b>CISSP® ISSAP</b> * <b>Information Systems Security Architecture Professional</b></p> <p>CISSP 취득 후 2년 이상의 업무경력 필요 ANAB(ISO/IEC표준 17029) U.S.DoD 8570.1(국방부승인)</p> <p>[시험과목] 1. Architect for Governance, Compliance and Risk Management 2. Security Architecture Modeling 3. Infrastructure Security Architecture 4. Identity and Access Management (IAM) Architecture 5. Architect for Application Security 6. Security Operations Architecture</p>	<p style="text-align: center;"><b>CISSP® ISSEP</b> * <b>Information Systems Security Engineering Professional</b></p> <p>CISSP 취득 후 2년 이상의 업무경력 필요 ANAB(ISO/IEC표준 17030) U.S.DoD 8570.1(국방부승인)</p> <p>[시험과목] 1. Systems Security Engineering Foundations 2. Risk Management 3. Security Planning and Design 4. Systems Implementation, Verification and Validation 5. Secure Operations, Change Management and Disposal</p>

<p style="text-align: center;"><b>CISSP® ISSMP</b> * <b>Information Systems Security Management Professional</b></p> <p>CISSP 취득 후 2년 이상의 업무경력 필요 ANAB(ISO/IEC표준 17031) U.S.DoD 8570.1(국방부승인)</p> <p>[시험과목]</p> <ol style="list-style-type: none"> <li>1. Leadership and Business Management</li> <li>2. Systems Lifecycle Management</li> <li>3. Risk Management</li> <li>4. Threat Intelligence and Incident Management</li> <li>5. Contingency Management</li> <li>6. Law, Ethics, and Security Compliance Management</li> </ol>	<p style="text-align: center;"><b>CSSLP®</b> * <b>Certified Secure Software Lifecycle Professional</b></p> <p>4년 이상 업무경력 필요 ANAB(ISO/IEC표준 17027) U.S. DoD 8570.1(국방부승인)</p> <p>[시험과목]</p> <ol style="list-style-type: none"> <li>1. Secure Software Concepts</li> <li>2. Secure Software Requirements</li> <li>3. Secure Software Architecture and Design</li> <li>4. Secure Software Implementation</li> <li>5. Secure Software Testing</li> <li>6. Secure Software Lifecycle Management</li> <li>7. Secure Software Deployment, Operations, Maintenance</li> <li>8. Secure Software Supply Chain</li> </ol>	<p style="text-align: center;"><b>SSCP®</b> * <b>Systems Security Certified Practitioner</b></p> <p>4년 이상 업무경력 필요 ANAB(ISO/IEC표준 17027) U.S. DoD 8570.1(국방부승인)</p> <p>[시험과목]</p> <ol style="list-style-type: none"> <li>1. Security Operations and Administration</li> <li>2. Access Controls</li> <li>3. Risk Identification, Monitoring and Analysis</li> <li>4. Incident Response and Recovery</li> <li>5. Cryptography</li> <li>6. Network and Communications Security</li> <li>7. Systems and Application Security</li> </ol>
---	--	--

<표 2-33> ISACA 운영 자격증

<p style="text-align: center;"><b>CISA®</b> * <b>Certified Information Systems Auditor</b></p> <p>응시자들은 시험 합격 후, 관련 경력을 쌓아 CISA 인증을 5년 이내에 신청할 수 있음 [시험과목]</p> <ol style="list-style-type: none"> <li>1. Information Systems Auditing Process (21%)</li> <li>2. Governance &amp; Management of IT (17%)</li> <li>3. Information Systems Acquisition, Development &amp; Implementation (12%)</li> <li>4. Information Systems Operations (23%)</li> <li>5. Protection of Information Assets (27%)</li> </ol>	<p style="text-align: center;"><b>CISM®</b> * <b>Certified Information Security Manager</b></p> <p>응시자들은 시험 합격 후, 관련 경력을 쌓아 CISM 인증을 5년 이내에 신청할 수 있음 [시험과목]</p> <ol style="list-style-type: none"> <li>1. Information Security Governance (17%)</li> <li>2. Information Security Risk Management (20%)</li> <li>3. Information Security Program (33%)</li> <li>4. Incident Management (30%)</li> </ol>	<p style="text-align: center;"><b>CRISC®</b> * <b>Certified in Risk and Information Systems Control</b></p> <p>관련 자격 인증 시험 우선 통과 필요 [시험과목]</p> <ol style="list-style-type: none"> <li>1. Governance (26%)</li> <li>2. IT Risk Assessment (20%)</li> <li>3. Risk Response and Reporting (32%)</li> <li>4. Information Technology and Security (22%)</li> </ol>
<p>평균 연봉 149,000 달러(미국) 현재 자격증 보유자 15.1만+</p>	<p>평균 연봉 149,000 달러(미국) 현재 자격증 보유자 4.8만+</p>	<p>평균 연봉 151,000 달러(미국) 현재 자격증 보유자 3만+</p>
<p style="text-align: center;"><b>CDPSE®</b> * <b>Certified Data Privacy Solutions Engineer</b></p> <p>관련 자격 인증 시험 우선 통과 필요 [시험과목]</p> <ol style="list-style-type: none"> <li>1. Privacy Governance (Governance, Management &amp; Risk Management) (34%)</li> <li>2. Privacy Architecture (36%)</li> <li>3. Data Lifecycle (30%)</li> </ol>	<p style="text-align: center;"><b>CGEIT®</b> * <b>Certified in the Governance of Enterprise IT</b></p> <p>관련 자격 인증 시험 우선 통과 필요 [시험과목]</p> <ol style="list-style-type: none"> <li>1. Governance of Enterprise IT (40%)</li> <li>2. IT Resources (15%)</li> <li>3. Benefits Realization (26%)</li> <li>4. Risk Optimization (19%)</li> </ol>	<p style="text-align: center;"><b>CSX-P®</b> * <b>CSX Cybersecurity Practitioner</b></p> <p>운영 종료</p> <p>그러나, 여전히 자격증 보유자들은 보안 전문성을 인정받고 있음</p>
<p>평균 연봉 150,000 달러(미국) 현재 자격증 보유자 1.6만+</p>	<p>평균 연봉 141,000 달러(미국) 현재 자격증 보유자 8천+</p>	<p style="text-align: center;">-</p>



- 검정 항목이 정보보안 관리 및 컴플라이언스부터 시스템/네트워크 보안 관리, 어플리케이션 보안까지 전반을 다루기에 범주가 너무 넓고, 관리적 정보보안에 특화된 자격도 아니며, 위험관리는 하위 세세항목의 하나로만 포함
- 민간 자격제도 중에서는 개인정보에 관심이 높아 CPPG(공인민간)에 대한 수요가 높은 편이며, 민간자격으로 등록되지는 않았으나 ISMS-P 인증심사원과 PIA(개인정보 영향평가 전문인력)가 실제 업무 현장에서의 활용도가 높은 것으로 알려져 있음
  - ISMS-P, PIA는 현업에서 실무경험이 오랜 경력자들이 경험을 토대로 하여 취득
  - 자격 취득을 위한 요구조건이 높고 시험 난이도가 높은 편으로 알려져 있음
- 국외 정보보호 분야 주요 자격제도 중 정보보호 관리 역량을 포괄하는 자격제도는 검정 항목으로 ‘위험 관리 및 평가’를 포함
  - 미국 NICE Framework(사이버보안 분야 업무분류체계)의 첫 번째 카테고리인 “안전한 보급”의 첫 번째 업무 역할은 “위험관리”이며, NICCS에서 제공하는 커리어패스에서 제공하는 대표 사이버보안 업무 지식(Top Skills) 9개 중 하나가 위험관리(Risk Assurance and Management)
  - 영국은 CyBOK(사이버보안 분야 지식분류체계) 개발을 통해 사이버보안을 정의. 첫 번째 분야는 “조직 및 제도적 측면”이며 위험관리(Risk Management & Governance)를 포함
  - 실제 정보보호 실무를 함에 있어, 조직 내 거버넌스 체계의 안정성 확보와 즉각적인 사고 대응을 위해서는 위험관리 체계가 잡혀 있어야 하며, 실무자들은 충분히 훈련되어 있어야 함
  - 실질적으로, 위험 관리 및 평가는 정보보안 관리의 핵심 업무이자 숙련도를 요하는 업무이며, 전반적인 정보보안 관리 역량 평가에 필수적인 항목
  - 전산·IT·소프트웨어 등의 업무와는 차별화되면서, 정보보호 관리 업무 전반을 포괄적으로 커버할 수 있고, 보안 관리 업무에 관심있는 인력에게 필요한 자격제도 개설 필요
- 위험관리는 조직의 정보보호 관리 활동의 핵심이라 할 수 있으며, 전문적인 시스템 및 네트워크 보안운영 스킬을 보유한 엔지니어와는 달리, 위험관리 전문가는 정보보호 및 개인정보 보호를 위한 기술적 조치에 대한 포괄적인 이해를 기반으로, 조직을 둘러싼 정보보호 및 개인 정보 보호 환경을 파악하고 조직 외부에서 요구하는 컴플라이언스를 담당하여 최고의사결정자를 이해시켜 설득하고 조직의 위험을 감수 가능한 수준으로 낮추는 업무를 수행하는 인력
  - 조직을 정보보호 및 개인정보보호 관점에서 총체적으로 바라보고 설명할 수 있는 인력임

- 위험관리(Risk Management)란 조직의 자산에 대한 위험을 감수할 수 있는 수준으로 유지하기 위하여 자산에 대한 위험을 분석하고 이러한 위험으로부터 자산을 보호하기 위한 비용 대비 효과적인 보호대책을 마련하는 일련의 과정을 말함<sup>38)</sup>
  - 일반적으로 전략과 계획을 수립하고, 위험을 구성하는 요소들을 분석하고, 이러한 분석에 기초하여 위험을 평가하여, 필요한 정보보호 대책을 선정하고, 이들을 구현할 계획을 수립하는 절차로 이루어짐
  - 과거에는 위험관리를 정보보호 관리의 전 과정을 포함하는 사이클로 정의한 경우도 있으나, 최근에는 일부를 제외하고는 정보보호 관리과정에 위험관리가 포함되는 것으로 봄
- ISO/IEC 27001(2013)에서는 ISMS(정보보호관리체계)의 범위 및 문맥에서 구현될 통제 항목이 위험 분석에 기반할 필요가 있다고 명시<sup>39)</sup>
  - 위험 분석의 목적은 조직의 위험을 수용 가능한 수준으로 관리하는 것으로 정의하는데, 여기서 ‘수용 가능한 위험’이란 조직의 경영 목적을 달성하는 데 방해가 되지 않는 위험으로, 조직은 모든 위험에 대응할 수 없으므로 수용 가능한 위험의 수준을 정의하여 위험의 수준이 낮은 경우에는 위험을 감수하게 됨.
  - 위험관리는 ISMS에서 다루어지는 핵심 프로세스 중의 하나
- NIST(미국국립표준기술연구소)는 위험관리(Risk Management)를 조직의 미션 달성과 비즈니스 계획 활동, 기업 아키텍처, SDLC 프로세스, 시스템 수명 주기 프로세스에 필수적인 시스템 엔지니어링 활동 등 조직의 모든 측면에 영향을 미치는 총체적인 활동으로 정의<sup>40)</sup>
  - 조직 차원에서 적절한 위험관리를 준비하지 않으면, 정보보호 및 개인정보 보호 활동에 지나치게 많은 비용이 소요되고, 숙련된 정보보호 및 개인정보 보호 전문가를 적재적소에 제대로 활용할 수가 없어, 비효율적인 솔루션이 나올 수 있음
- 사이버위험관리전문가 자격제도는 정보보호 관리의 핵심적인 역할을 할 사이버 위험관리 전문가를 키울 자격제도로써 정부의 2026년까지 신규 인력 4만 명, 재직자 6만 명 등 총 10만 명의 사이버보안 인재를 육성한다는 계획<sup>41)</sup>에 기여할 수 있을 것

38) 한국인터넷진흥원 (2004), 정보보호 위험관리 가이드라인 [수탁기관 : 한국정보시스템감사통제협회]

39) 황성운 (2018), 정보 보안 원리 및 실습, 생능출판사, pp.577-597.

40) NIST (2020), Risk Management Framework for Information Systems and Organizations : A System Life Cycle Approach for Security and Privacy, NIST Special Publication 800-37 Revision 2, PP.6-10.

41) 과학기술정보통신부 보도참고자료 (2022.07.13.), ‘사이버 10만 인재 양성 방안’ 발표.

(2) (신설) 사이버보안수학능력평가 (Cyber Literacy Generalist, CLG)

<p>(신설) 사이버보안수학능력평가 Cyber Literacy Generalist (CLG)</p>	<p>▶ 정보보호에 관심을 가지고 기초지식을 습득하길 원하는 과정에서 준비 또는 보유한 기초지식의 수준을 평가할 수 있는 수준의 자격제도 ▶ 초급자 레벨</p>
---	---

- 현재 국내 자격 중에는 정보보호에 관심을 가지고 기초 지식을 쌓고 평가받기를 원하는 수준의 초급자 역량을 검증할 수 있는 자격제도가 없음
  - 초보자들을 위한 자격제도는 정보보호 분야의 관심을 높이거나, 자신이 가진 관심이 실제 업무역량 향상을 위한 밑거름이 될만한지를 가름할 수 있는 잣대가 됨
  - 개인의 정보보호 리터러시 수준을 검증할 수 있는 자격제도가 있다면 정보보호에 대한 관심도를 높이고 자신의 수준을 점검해가며 학습 단계를 높여나가고 나아가 직업으로까지 고려할 수 있는 직무 로드맵을 수립하는 데에는 도움을 줄 수 있을 것
- 사이버보안수학능력평가 자격제도는 기본적으로는 사이버 공간에서의 리터러시 교육을 목적으로 함. 이와 더불어, 디지털 기술과 사이버 공간에 대한 이해, 안전한 사이버 공간을 만들기 위해 필요한 정보보호 및 개인정보 보호의 범주와 방법에 대해 사용자 입장에서의 기초적인 지식 수준을 평가하는 것을 목표로 하여, 궁극적으로 청소년 및 정보보호에 관심을 두고 있는 이들이 정보보호 업무 수행 인력으로서 진로를 잡을 수 있도록 발판이 될 수 있도록 하고자 함
- OECD-PISA의 조사보고서에 따르면, 우리나라 학생들의 읽기 능력은 OECD 평균보다 높지만, 의견과 사실을 구분하는 능력은 최하위권으로 나타나, 대한민국 디지털 문해력이 위기에 처해 있는 상황 <그림 2-1 참조><sup>42)</sup>
  - 이에 정부는 ‘디지털 신기술을 개발·활용·운용하는데 필요한 지식과 역량을 갖춘 인재’를 디지털 인재로 정의하고, 100만 디지털 인재양성 계획을 추진 중<sup>43)</sup>
- 사이버보안수학능력평가 자격제도는 대한민국 국민의 디지털 리터러시 수준을 함양시키고, 지능정보사회에서 무엇보다도 중요한 내정보 지키기와 디지털 기술 제대로 사용하기를 주체적으로 수행할 수 있는 자기 능력을 함양시킬 수 있는 역할을 할 것

42) OECD (2021), 21st-Century Readers DEVELOPING LITERACY SKILLS IN A DIGITAL WORLD.

43) 관계부처 합동 (2022), 디지털 인재양성 종합방안.

## 2. 국가직무능력표준과의 관계

- 사이버위험관리전문가(Cyber Risk Management Specialist, CRMS)는 국가직무능력표준의 세분류인 「정보보호관리·운영」과 「개인정보보호관리·운영」에 해당하는 직무를 수행하는 데 필요한 정보보호 관리 분야의 지식 및 기술을 검정하는 것을 목적으로 함
- 사이버보안수학능력평가(Cyber Literacy Generalist, CLG)는 (개인)정보보호관리·운영으로 진입하고자 하는 인력이 현재의 학습 수준을 평가하여 학습 척도로 삼을 수 있도록 하고자 함
- 세분류 ‘정보보호관리·운영’의 능력단위는 <표 2-35>와 같음
  - 정보보호관리·운영은 조직의 비전과 미션을 수행하기 위하여 정보 자산을 안정적으로 운영하는 데 필요한 정보보호 전략과 정책을 수립하고, 법령 준수, 보호관리 활동을 수행하며, 위험관리에 기반한 정보보호 대책을 도출하고 실행하는 일

<표 2-35> 한국직무능력표준(NCS) 직무능력단위 : 정보보호관리·운영

NCS 웹사이트 최종 접속일 : 2023.11.19.

순번	능력단위명	능력단위요소	수준
1	정보보호 거버넌스 구현	정보보호 전략 수립하기 / 정보보호 자원 할당하기	8
2	정보보호 정책 기획	정보보호 정책 수립하기 / 정보보호 정책 유지관리하기	7
3	보안 위험관리	위험관리 계획 수립하기 / 위험 분석하기	7
4	정보보호 계획 수립	정보보호 목표 설정하기 / 정보보호 대상 범위 설정하기	6
5	네트워크 보안 운영	네트워크 보안솔루션 운영하기 네트워크 보안솔루션 운영 개선하기	5
6	애플리케이션 보안 운영	애플리케이션 보안솔루션 운영하기 애플리케이션 보안솔루션 운영 개선하기	5
7	시스템 보안 운영	시스템 보안솔루션 운영하기 시스템 보안솔루션 운영 개선하기	5
8	관리적 보안 운영	정보보호 인식제고 교육하기 / 정보보호 이행 점검하기	5
9	물리 보안 운영	물리 보안솔루션 운영하기 물리 보안솔루션 운영 개선하기	5
10	보안 장비 운용	보안시스템 상태 체크하기 / 정책요청 적용하기	3
11	보안성 검토	보안성 검토 기준 수립하기 / 보안성 검토 수행하기	7
12	내부 보안 감사 수행	보안 감사 계획 수립하기 / 보안 감사 실행하기	7
13	협력사 보안 관리	협력사 보안 정책 수립하기 / 협력사 보안 운영하기	6

- 기존에 정보통신(대분류) - 정보기술(중분류) - 정보보호(소분류) 세분류의 하나로 분류되어 있던 ‘개인정보보호’를 소분류로 올리는 작업을 진행 중이나, 공개 전 (23년11월말기준)
  - 개인정보보호(소분류)의 세분류는 개인정보보호관리·운영, 개인정보가명익명처리, 개인정보 인증평가 3개로 예정됨
- 기존 세분류 ‘개인정보보호’의 능력단위는 <표 2-36>과 같음
  - 개인정보보호란 개인정보를 법령 등에 따라 생명주기별로 안전하게 보호하고 관리·운영하기 위한 기술적, 물리적, 관리적 보호조치를 수행하는 일

<표 2-36> 한국직무능력표준(NCS) 직무능력단위 : 개인정보보호

NCS 웹사이트 최종 접속일 : 2023.11.19.

순번	능력단위명	능력단위요소	수준
1	개인정보보호 법령정책 분석	개인정보보호 관련 법령·정책 수집하기 개인정보보호 관련 법령·정책 분석하기	6
2	개인정보보호 기획	개인정보보호 목표 설정하기 개인정보보호 범위 설정하기	8
3	개인정보 영향평가 관리	개인정보 영향평가 계획 수립하기 개인정보 영향평가 수행하기	7
4	개인정보보호 위험관리	개인정보보호 위험관리 계획 수립하기 개인정보보호 위험 분석평가하기	7
5	개인정보보호 운영	개인정보 처리시스템 운영하기 개인정보 사고 대응하기	5
6	개인정보보호 활동 모니터링	개인정보보호 활동 모니터링 계획 수립하기 내부 정보보호 활동 모니터링 하기	6
7	개인정보보호 관리체계 인증	개인정보보호 관리체계 인증 체계 수립하기 개인정보보호 관리체계 인증 기준 수립하기	7
8	개인정보보호 감사	개인정보보호 감사 계획 수립하기 개인정보보호 감사 실행하기	7

- 사이버위험관리전문가(Cyber Risk Management Specialist, CRMS), 사이버보안수학능력평가 (Cyber Literacy Generalist, CLG)의 직무내용이자 출제기준을 NCS 세분류 및 직무능력단위와 매칭한 결과는 <표 2-37>과 같음
  - 사이버보안수학능력평가(CLG)는 주요 시험대상을 주니어(중·고등학생 및 비전공 대학생 등)로 하므로 직무수행에 필요한 역량을 검증하는 자격증은 아님

<표 3-37> 한국직무능력표준(NCS) 직무능력단위와 신규 민간자격과의 관계

NCS 세분류	NCS 능력단위	사이버위험관리전문가 (Cyber Risk Management Specialist, CRMS)	사이버보안수학능력평가 (Cyber Literacy Generalist, CLG)
정보보호 관리·운 영	정보보호 거버넌스 구현	○	×
	정보보호 정책 기획	○	×
	보안 위험관리	○	○
	정보보호 계획 수립	○	×
	네트워크 보안 운영	△	△
	애플리케이션 보안 운영	△	×
	시스템 보안 운영	△	△
	관리적 보안 운영	○	○
	물리 보안 운영	△	×
	보안 장비 운용	△	×
	보안성 검토	△	×
	내부 보안 감사 수행	○	×
	협력사 보안 관리	○	×
개인 정보보호	개인정보보호 법령·정책 분석	○	△
	개인정보보호 기획	○	△
	개인정보 영향평가 관리	△	×
	개인정보보호 위험관리	○	○
	개인정보보호 운영	△	×
	개인정보보호 활동 모니터링	△	×
	개인정보보호 관리체계 인증	○	○
	개인정보보호 감사	○	×

○ : 해당함 △ : 일부 해당 (기술적인 조치는 제외하기 때문) × : 해당하지 않음

### 3. 관련 학과/전공 및 인력 수요 규모

- CRMS는 4년 대학 졸업(예정)자 또는 이와 동등 이상의 학력이 있다고 인정되는 자<sup>44)</sup>라면 누구나 응시 가능하며, 진출 가능한 직무는 ‘정보보안 관리’
  - 한국직무능력표준(NCS) 직무능력단위 중 「정보보호관리·운영」에 해당
  - 응시할 수 있는 전공을 제한하지는 않으나, 참고로 국내 4년제 대학 정보보호 관련학과 현황은 <표 2-38>과 같음
  - 각 학과/전공에서 운영 중인 교과목 중 CRMS 자격제도의 시험 준비와 관련이 높은 교과목은 정보보호(안) 윤리/법제도/규정, 정보보호(안) 관리, 정보보호(안) 관리체계 구축, 정보보호(안) 신기술 등으로 상세 정보는 <표 2-39>과 같음

<표 2-38> 2022년 국내 4년제 대학 정보보호 관련 학과 개설 현황

대학교명	학과명	재적학생 수 (명)
가천대학교	컴퓨터공학부(스마트보안전공)	50
건양대학교	사이버보안학과	41
경남대학교	컴퓨터보안전공	74
경희사이버대학교	AI사이버보안전공	77
고려대학교	사이버국방학과	114
	스마트보안학부	56
고려대학교(세종)	인공지능사이버보안학과	130
광주대학교	사이버보안경찰학과	53
국민대학교	정보보안암호수학과	175
단국대학교	산업보안학과	67
대구카톨릭대학교	사이버보안전공	120
대구대학교	컴퓨터정보공학부(정보보호전공)	61
대전대학교	정보보안학과	167
덕성여자대학교	사이버보안전공	59
동국대학교	융합보안학과	165
동명대학교	정보보호학과	132
동서대학교	정보보안학과	116
동신대학교	정보보안학과	126
목포대학교	정보보호학과	139
	컴퓨터·정보보호학부	22

44) 국가기술자격법 시행령 [별표4의2] 기술·기능 분야 국가기술자격의 응시자격(제14조제7항 관련)

대학교명	학과명	재적학생 수 (명)
배재대학교	정보보안학전공	89
상명대학교	정보보안공학과	163
서울디지털대학교	정보보안전공	51
서울사이버대학교	빅데이터·정보보호학과	451
서울여자대학교	정보보호학과	366
성신여자대학교	융합보안공학과	328
세종대학교	정보보호학과	140
세종사이버대학교	정보보호학과	292
수원대학교	정보보호전공	171
순천향대학교	정보보호학과	249
아주대학교	사이버보안학과	187
영산대학교	사이버보안학과	37
우석대학교	정보보안학과	134
우송대학교	IT융합학부 컴퓨터정보·보안전공	223
위덕대학교	경찰정보보안학과	95
유원대학교	정보통신보안학과	117
이화여자대학교	사이버보안전공	139
제주국제대학교	정보보안공학과	13
조선대학교	정보통신공학부(정보보안전공)	93
중부대학교	정보보호학전공	202
중앙대학교	산업보안학과	183
청주대학교	디지털보안전공	120
한국해양대학교	해사인공지능·보안학부	61
한세대학교	산업보안학과	109
한양사이버대학교	해킹보안학과	325
합계	45개 학과/전공	6,282

출처 : 국가정보원 등 (2023.5), 2023 국가정보보호백서, pp.192-193.

<표 2-39> 2022년 국내 4년제 대학 정보보호 관련 학과의 CRMS 관련 교과목

(주의사항 1) 각 홈페이지에서는 ‘교과목명’에 대한 정보만 공개되어 있으며, 상세 내용을 확인할 수가 없으므로 담당 교수에 따라 수업내용과 주교재가 교과목명과 다를 수 있음

(주의사항 2) 국내 정보보호 학과/전공은 공학교육인증 등을 시행하고 있지 않으므로(일부 공과대학에 설치된 학과/전공은 공학교육인증을 따름) 교과목 운영에 표준이 없음. 이에, 교과목명이 같더라도 수업내용은 교수자나 학교마다 다를 수 있으며, 반대로 교과목명이 완전히 다르더라도 수업내용은 같을 수도 있음

(주의사항 3) 본 표는 참고용으로 작성한 것이며, 해당 학과/전공의 실제 운영과 다를 수 있음

\* 각 대학 홈페이지 최종 접속일자 : 2023.12.17.

대학교명	학과명	관련 교과목
가천대학교	컴퓨터공학부(스마트보안전공) <a href="https://www.gachon.ac.kr/ai-security/8189/subview.do">https://www.gachon.ac.kr/ai-security/8189/subview.do</a>	(4학년) 정보보호 정책 (4학년) 정보보호 컨설팅
건양대학교	사이버보안학과 <a href="https://sec.konyang.ac.kr/prog/curriculum/sec/sub03_02/primecics4/view.do">https://sec.konyang.ac.kr/prog/curriculum/sec/sub03_02/primecics4/view.do</a>	(2학년) 개인정보 안전성 확보조치 (3학년) 개인정보 법제도와 정책 (3학년) 개인정보 영향평가 (4학년) 정보보호 및 개인정보보호 관리체계
경남대학교	컴퓨터보안전공 <a href="https://www.kyungnam.ac.kr/ce/3667/subview.do">https://www.kyungnam.ac.kr/ce/3667/subview.do</a>	(2학년) 정보보안개론
경희사이버대학교	AI사이버보안전공 <a href="https://www.khcu.ac.kr/sub/tab.do?MENU_SEQ=200036134&amp;TAB_SEQ=200125264">https://www.khcu.ac.kr/sub/tab.do?MENU_SEQ=200036134&amp;TAB_SEQ=200125264</a>	(3학년) IT거버넌스와 정보보호 관리체계 (4학년) 정보보호법 제도
고려대학교	사이버국방학과 <a href="https://gss.korea.ac.kr/ime/info/cyber.do">https://gss.korea.ac.kr/ime/info/cyber.do</a>	교과목 정보 없음
	스마트보안학부 <a href="https://gss.korea.ac.kr/ime/info/smart.do">https://gss.korea.ac.kr/ime/info/smart.do</a>	(전공선택) 위협관리 (전공선택) 사이버기술과 법 (전공선택) 개인정보보호
고려대학교(세종)	인공지능사이버보안학과 <a href="https://aisecu.korea.ac.kr/">https://aisecu.korea.ac.kr/</a>	(4학년) 사이버법과 정책 (4학년) 정보보호 법제 특론 (4학년) 정보보호 위협 관리 평가
광주대학교	사이버보안경찰학과 <a href="https://cyfo.gwangju.ac.kr/bbs/board.php?bo_table=b0102">https://cyfo.gwangju.ac.kr/bbs/board.php?bo_table=b0102</a>	(3학년) 정보보호법
국민대학교	정보보안암호수학과 <a href="https://cst.kookmin.ac.kr/security/curriculum">https://cst.kookmin.ac.kr/security/curriculum</a>	* 수학과 교육과정
단국대학교	산업보안학과 <a href="https://www.dankook.ac.kr/web/kor/-183">https://www.dankook.ac.kr/web/kor/-183</a>	(3학년) 정보보호 이론 (3학년) 기술과 경영
대구카톨릭대학교	사이버보안전공 <a href="http://software.cu.ac.kr/?menu_code=213">http://software.cu.ac.kr/?menu_code=213</a>	(2학년) 사이버 보안정책 (4학년) 정보보호 관리체계 구축 (4학년) 해킹과 바이러스 (4학년) 침입탐지와 방지

대학교명	학과명	관련 교과목
대구대학교	컴퓨터정보공학부(정보보호전공) <a href="https://infosec.daegu.ac.kr/hakgwa_home/infosec/index.php">https://infosec.daegu.ac.kr/hakgwa_home/infosec/index.php</a>	(3학년) 국가사이버안보의 이해 (4학년) 사이버 침해사고 및 대응 (4학년) 정보보호 신기술
대전대학교	정보보안학과 <a href="https://www.dju.ac.kr/dcis/cm/cntnts/cntntsView.do?mi=1987&amp;cntntslid=1458">https://www.dju.ac.kr/dcis/cm/cntnts/cntntsView.do?mi=1987&amp;cntntslid=1458</a>	교과목 정보 없음
덕성여자대학교	사이버보안전공 <a href="https://www.duksung.ac.kr/cybersec/contents/contents.do?cildx=2175&amp;menuid=3314">https://www.duksung.ac.kr/cybersec/contents/contents.do?cildx=2175&amp;menuid=3314</a>	* 포렌식, 해킹 등 기술 중심
동국대학교	융합보안학과 <a href="https://security.dongguk.edu/ibuilder.do?per_menu_idx=22&amp;menu_idx=27&amp;tabCnt=3">https://security.dongguk.edu/ibuilder.do?per_menu_idx=22&amp;menu_idx=27&amp;tabCnt=3</a>	* 범죄 수사 교육과정
동명대학교	정보보호학과 <a href="https://www.tu.ac.kr/is/sub02_03.do">https://www.tu.ac.kr/is/sub02_03.do</a>	(4학년) 개인정보 보호체계 (4학년) 정보보호 컨설팅 (4학년) 정보보호 세미나
동서대학교	정보보안학과 <a href="https://uni.dongseo.ac.kr/ictsecurity/index.php?pCode=MN2000046">https://uni.dongseo.ac.kr/ictsecurity/index.php?pCode=MN2000046</a>	* 포렌식, 해킹 등 기술 중심
동신대학교	정보보안학과 <a href="https://is.dsu.ac.kr/is/index.php?pCode=course&amp;mode=view&amp;idx=1374">https://is.dsu.ac.kr/is/index.php?pCode=course&amp;mode=view&amp;idx=1374</a>	(4학년) 정보보안 윤리 (4학년) 정보보호 관리와 법규
목포대학교	정보보호학과(컴퓨터학부 정보보호전공) <a href="https://secu.mokpo.ac.kr/secu/10904/subview.do">https://secu.mokpo.ac.kr/secu/10904/subview.do</a>	(2학년) 정보보호 법과 윤리 (4학년) 보안감사
	컴퓨터 · 정보보호학부	-
배재대학교	정보보안학전공 <a href="https://hakgwa.pcu.ac.kr/security/contents/243">https://hakgwa.pcu.ac.kr/security/contents/243</a>	(1학년) 사이버 사회 이해 (3학년) 사이버보안 관리 법규
상명대학교	정보보안공학과 <a href="https://dis.smu.ac.kr/dis/admission/information.do">https://dis.smu.ac.kr/dis/admission/information.do</a>	(4학년) 정보보호 관리 평가
서울디지털대학교	정보보안전공 <a href="http://security.sdu.ac.kr/security/cms/FR_CON/index.do?MENU_ID=70">http://security.sdu.ac.kr/security/cms/FR_CON/index.do?MENU_ID=70</a>	(1학년) 정보보안 관리 및 법규 (2학년) 정보관리 역량 강화 (3학년) 정보보호 위험 관리 (3학년) CISSP 전문가 과정
서울사이버대학교	빅데이터 · 정보보호학과 <a href="https://www.iscu.ac.kr/03_aboutschool/27_03_training.asp">https://www.iscu.ac.kr/03_aboutschool/27_03_training.asp</a>	(2학년) 개인정보보호 (3학년) 사이버보안 (4학년) 정보보안 관리 및 법규
서울여자대학교	정보보호학과 <a href="https://www.swu.ac.kr/www/futured_3.html">https://www.swu.ac.kr/www/futured_3.html</a>	(3학년) 개인정보 보호법의 이해 (3/4학년) 개인정보 보호 정책 및 관리적 보호조치 (ISMS-P) (3/4학년) 개인정보 기술적 보호 조치 (4학년) 정보보호 산업 기술 최신동향 (4학년) 정보보호 관리체계 인증

대학교명	학과명	관련 교과목
성신여자대학교	융합보안공학과 <a href="https://www.sungshin.ac.kr/cse/index.do">https://www.sungshin.ac.kr/cse/index.do</a>	(2학년) 정보보호 법과 보안 정책 (3학년) 기업정보 보안관리 체계 (3학년) 보안성 평가 방법론 이외 법/제도적 관련 타전공 추천
세종대학교	정보보호학과 <a href="https://home.sejong.ac.kr/~isdpt/15.html">https://home.sejong.ac.kr/~isdpt/15.html</a>	* 수리학 등 공학인증 요건만 게시
세종사이버대학교	정보보호학과 <a href="https://dept.sjcu.ac.kr/information/index.do">https://dept.sjcu.ac.kr/information/index.do</a>	해킹보안 / 사이버수사 / 산업보안 / 보안코딩 등 4개 계열로 분리 [사이버수사 전문가 과정] 정보보호법 및 사이버 법률 정보보호 정책 [산업보안 전문가 과정] 정보보호 컨설팅 정보보호 정책 사이버 보안의 미래
수원대학교	정보보호전공 <a href="https://www.suwon.ac.kr/index.html?menu=1137">https://www.suwon.ac.kr/index.html?menu=1137</a>	(3학년) 정보보안 관리 I/II (4학년) 지적재산의 보호와 관리
순천향대학교	정보보호학과 <a href="https://home.sch.ac.kr/security/02/01.jsp">https://home.sch.ac.kr/security/02/01.jsp</a>	(4학년) 정보보호 법과 윤리 (4학년) 정보보호 현장 실무 (4학년) 정보보호 평가 관리 인증
아주대학교	사이버보안학과 <a href="https://security.ajou.ac.kr/security/edu/edu02.jsp">https://security.ajou.ac.kr/security/edu/edu02.jsp</a>	(1학년) 사이버보안 윤리 (2학년) 정보보호 법제도와 정책 (4학년) 사이버보안 사례 특강
영산대학교	사이버보안학과 <a href="https://security.yosu.ac.kr/security/CMS/Contents/Contents.do?mCode=MN022">https://security.yosu.ac.kr/security/CMS/Contents/Contents.do?mCode=MN022</a>	(4학년) 정보보호 관리체계 구축
우석대학교	정보보안학과 <a href="https://is.woosuk.ac.kr/2015/inner.php?sMenu=B1000">https://is.woosuk.ac.kr/2015/inner.php?sMenu=B1000</a>	(4학년) 정보보호법
우송대학교	IT융합학부 컴퓨터정보·보안전공 <a href="https://cs.wsu.ac.kr:444/main/intro.jsp">https://cs.wsu.ac.kr:444/main/intro.jsp</a>	* 컴퓨터공학 중심 교육과정 보안 교과목 소수
위덕대학교	경찰정보보안학과 <a href="https://hacking.uu.ac.kr/bbs/board.php?bo_table=su_b01_05">https://hacking.uu.ac.kr/bbs/board.php?bo_table=su_b01_05</a>	* 범죄 수사 교육과정 보안 교과목 소수
유원대학교	정보통신보안학과 <a href="https://info.u1.ac.kr/info/html/edu/0301.html">https://info.u1.ac.kr/info/html/edu/0301.html</a>	* 정보통신 교육과정 (2학년) 사이버 윤리
이화여자대학교	사이버보안전공 <a href="https://security.ewha.ac.kr/security/index.do">https://security.ewha.ac.kr/security/index.do</a>	교과목 정보 없음 (상세조회 가능하나, 출력안됨)
제주국제대학교	정보보안공학과 <a href="https://www.jeju.ac.kr/department/computer/guide/educate.htm">https://www.jeju.ac.kr/department/computer/guide/educate.htm</a>	(4학년) 정보보안 실무

대학교명	학과명	관련 교과목
조선대학교	정보통신공학부(정보보안전공) <a href="https://eie.chosun.ac.kr/ice/11133/subview.do">https://eie.chosun.ac.kr/ice/11133/subview.do</a>	* 정보통신공학 교육과정 교과목명이 <정보보호>
중부대학교	정보보호학전공 <a href="https://www.joongbu.ac.kr/menu.es?mid=f50301000000">https://www.joongbu.ac.kr/menu.es?mid=f50301000000</a>	(3학년) 정보보호 관리 (캡스톤) (4학년) 정보보호 법과 윤리
중앙대학교	산업보안학과 <a href="https://security.cau.ac.kr/contents.htm?id=univ_major">https://security.cau.ac.kr/contents.htm?id=univ_major</a>	(1학년) 디지털 비즈니스와 보안 (1학년) 법학개론 (2학년) 보안 커뮤니케이션 (2학년) 개인정보 활용과 보호 (3학년) 기술경영과 보호 (3학년) 산업보안 거버넌스 (3학년) 산업보안 컨설팅
청주대학교	디지털보안전공 <a href="https://www.cju.ac.kr/sec/selectTnHaksaCurriculumList.do?key=7980&amp;dept=2000001533&amp;">https://www.cju.ac.kr/sec/selectTnHaksaCurriculumList.do?key=7980&amp;dept=2000001533&amp;</a>	(3학년) 정보보안 정책 및 평가 (4학년) 정보보안 실무 (4학년) 최신 보안기술 동향
한국해양대학교	해사인공지능·보안학부 <a href="https://www.kmou.ac.kr/aisec/cm/cntnts/cntntsView.do?mi=4920&amp;cntntsId=4898">https://www.kmou.ac.kr/aisec/cm/cntnts/cntntsView.do?mi=4920&amp;cntntsId=4898</a>	* 포렌식, 해킹 등 기술 중심 * 해사로서의 기술 역량 배양 중심
한세대학교	산업보안학과 <a href="https://www.hansei.ac.kr/kor/517/subview.do">https://www.hansei.ac.kr/kor/517/subview.do</a>	(1학년) 법학 입문 (2학년) 산업보안 거버넌스와 경제 (3학년) 개인정보 보호법 (3학년) 산업보안 컨설팅 (4학년) 산업보안 윤리 (4학년) 산업보안 판례 연구
한양사이버대학교	해킹보안학과 <a href="https://www.hycu.ac.kr/user/maSnEx/goMain/30043/subject.do">https://www.hycu.ac.kr/user/maSnEx/goMain/30043/subject.do</a>	(2학년) 정보보호 관리 (4학년) 정보보호 관리체계 (4학년) 정보보호 법제도
합계	45개 학과/전공	

- 한국정보보호산업협회가 국가통계로서 조사하는 「정보보호산업 실태조사」의 결과를 기준으로 정보보안 분야 종사자 수는 약 2.3만 명임. 이는 정보보호 산업인력이라고 할 수 있음
- 정보보호산업 실태조사의 조사대상은 한국정보보호산업협회의 회원사 즉 정보보호 전문 산업체임
- 실제 정보보호 인력은 전체 산업에 산재해 있음. 일반기업이나 공공기관의 정보보호 전담 부서에서 근무하거나 전담인력으로 전체 기업(기관)의 보안관리를 맡아 수행하는 인력을 포함하는 조사결과는 아님
- 직무별로는 ‘정보보안 관리’ 인력이 전체 종사인력의 26%이며<표 2-40>, 경력기간 4년 미만의 인력이 전체의 30.7% <표 2-41>

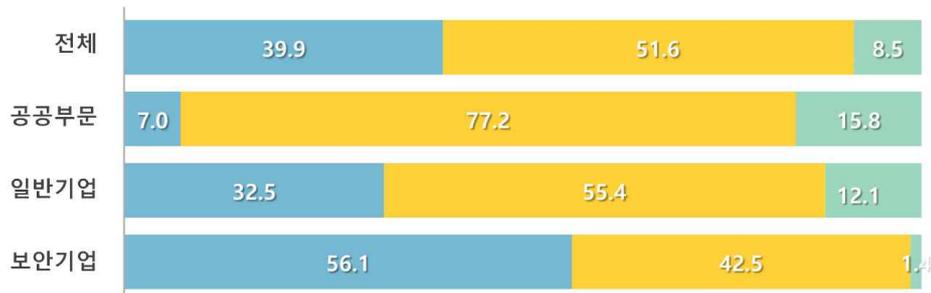
<표 2-40> 국내 정보보호산업체에 종사하는 정보보안 인력 현황 (직무별)

구분	인력 수	비율
정보보안 연구/개발자	6,294명	27.4%
엔지니어	7,291명	31.7%
정보보안 관리 : 정보보안 컨설팅	2,322명	10.1%
정보보안 관리 : 정보보안 관제	3,158명	13.7%
정보보안 관리 : 정보보안 관리자	497명	2.2%
정보보안 영업직	2,131명	9.3%
기타 정보보안 관련직	1,303명	5.7%
합계	22,997명	

<표 2-41> 국내 정보보호산업체에 종사하는 정보보안 인력 현황 (경력년수별)

	4년 미만	4년이상 7년미만	7년이상 11년미만	11년이상 15년미만	15년이상	합계
정보보안	7,054명 30.7%	6,300명 27.4%	4,805명 20.9%	2,642명 11.5%	2,196명 9.5%	22,997명

- 국가통계는 아니지만, 한국인터넷진흥원이 비정기적으로 조사하고 있는 「정보보호 인력 현황 조사」 결과에 따르면<sup>45)</sup>, 국내 정보보호 인력은 대략 13.8만 명 ('19년 13만 5,194명)
  - 공공부문 종사인력 4,808명, 일반기업 종사인력 85,112명, 보안기업(=정보보안+물리보안) 종사인력 48,648명
  - 직무별로는 보안제품 개발 39.9%, 보안관리 51.6%, 보안사고 대응 8.5% <그림 2-1>. 보안기업의 경우 보안 제품 및 서비스 공급사이므로 '보안제품 개발' 업무 종사자 비중이 높은 편이지만, 일반기업과 공공부문은 보안 제품 및 서비스를 구매하여 이용하는 수요자에 해당하므로, '보안 관리' 업무 종사자 비중이 높게 나타남
  - CRMS 자격제도는 '보안 관리' 업무 종사자들이 전문성 강화를 위한 교육의 효과를 측정하거나 업무 역량 강화를 위한 커리어캡 구축의 준비를 돕는 역할을 하게 될 것임



<그림 2-1> 직무별 정보보호 인력 현황 (단위 : %)

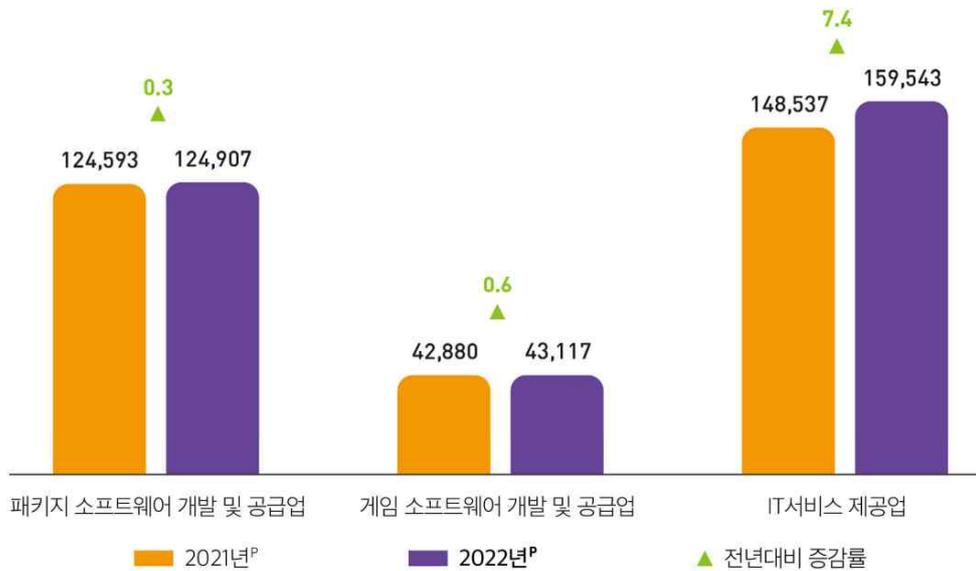
※출처 : 한국인터넷진흥원 (2022)

- 참고로 국가통계인 「ICT 인력동향 실태조사」를 통해 발표된 결과에 따르면<sup>46)</sup>, 2021년 국내 전체산업 인력은 2,493만 명이며, 이 중 ICT산업 인력은 108만 명
  - ICT산업 인력은 ICT산업(국가표준산업분류 기준 정보통신방송기기업, 정보통신방송서비스업, 소프트웨어 개발 및 제작업) 및 ICT관련산업(국가표준산업분류 기준 공사업, 유통업, 임대업, 수리업)의 상용 종사자를 말함
  - 정보보호(안)은 국가표준산업분류의 세세분류로도 분류되어 있지 않으나, 정보보호 산업인력(정보보호 전문업체 종사인력)의 경우 통상적으로 '소프트웨어 개발 및 제작업 중 IT서비스 제공업'에 포함되는 것으로 봄

45) 한국인터넷진흥원 (2022), 2022 정보보호 인력 현황조사.

46) 과학기술정보통신부, 한국정보통신진흥협회, 한국전자정보통신산업진흥원 (2023), 2022 ICT 인력동향실태조사.

- <그림 2-2>에서 볼 수 있는 바와 같이 IT서비스 제공업 종사인력 수는 상용 종사자 기준으로 2022년 현재 15.9만 명임



<그림 2-2> 2022년 소프트웨어 개발 및 제작업 인력 현황 (상용 종사자)(단위 : %)

출처 : 과학기술정보통신부, 한국정보통신진흥협회, 한국전자정보통신산업진흥원 (2023)

- CRMS 자격제도는 기본적으로 비관련학과 전공인 4년제 대학생(또는 졸업생)이 정보보호 업무에 관심을 두고 진로를 결정하는 데 있어 자신의 실력을 평가할 수 있는 바로미터의 역할을 하도록 하는 것을 신설 목표로 함
- 또한, 광범위한 정보통신 및 소프트웨어 업무 종사인력 중 경력개발의 방향을 정보보호(안)으로 설정하려는 경우, 역시 가장 기본적으로 갖춰야 할 또는 본인의 정보보호(안)에 대한 지식 정도를 가늠할 수 있는 척도로 활용하도록 할 수 있을 것으로 기대

### 제 3 절 공인민간자격 등록방안

○ 정보보호 분야 신규 민간자격 2종의 개요는 <표 2-42>와 같음

<표 2-42> 정보보호 관련 신규 민간자격 2종 개요

자격명	사이버위험관리전문가 Cyber Risk Management Specialist (CRMS)	사이버보안수학능력평가 Cyber Literacy Generalist (CLG)
등급	등급 없음	등급 없음
검정기준	사이버위험관리 전문가로서 갖추어야 할 지식에 대한 검정과 실무에 적용할 수 있는 능력을 검정	사이버보안 관련 기초지식의 습득 정도를 검정
직무내용	조직의 정보자산을 식별하고 적절한 보안대책(통제방안)을 구현하여 조직이 감내할만한 수준으로 위험을 관리하고, 경영진에게 보안 위험관리(분석·평가 포함)를 설명하고 설득할 수 있다.	국가직무능력표준의 「정보보호관리·운영」과 「개인정보보호관리·운영」에 해당하는 지식 및 기술에 대한 기초소양을 측정한다.
검정방법	필기 : 80문항, 객관식 택일형 실기 : 5문항, 필답형	필기 : 80문항, 객관식 택일형
응시자격	4년제 대학 졸업자 또는 졸업예정자 (전공 무관, 경력자의 경우 직무 분야 무관) 및 이에 상응하는 조건	나이·학력·전공·실무경력 제한 없음
시험시간	필기 : 120분 실기 : 90분	필기 : 120분
합격기준	필기 : 과목별 40점 이상, 전체 60점 이상 실기 : 과목 통합 60점 이상	수준 평가 (800점 만점)
검정 수수료	필기 : 100,000원 (*재학생 50% 할인) 실기 : 100,000원	필기 : 30,000원
자격증 발급비	10,000원 *온라인 무료 다운로드	10,000원 *온라인 무료 다운로드

- 2개 자격제도 모두 민간자격으로서 등급은 구분 없음. CRMS는 국가자격인 정보보안기사를 상급 자격제도로 하고, 그 아래의 수준을 평가하는 수준으로 설정함. 단, 정보보안기사는 정보보호(안) 기술에 대한 평가 비중이 높지만, CRMS는 정보보호(안) 관리 방법에 초점을 맞추어 평가함
- CRMS는 국가직무능력표준을 기준으로 「정보보호관리·운영」 직무의 수행과 관련이 있으며, CLG는 직접적인 직무능력 평가 제도는 아님
- 2개의 민간자격 모두 특별한 학력이나 경력년수 등의 자격 제한 조건은 없음. 다만, CRMS는 수준 유지를 위해 4년제 대학 졸업자(예정자) 및 그에 상응하는 조건 이상의 학력 조건은 두되, 학과/전공은 상관없음
- **검정수수료는 타 자격제도 운영 현황<표 2-43>과 내부연구진 검토를 거쳐 설정.** CRMS는 직무 수행(예정)자를 대상으로 시험을 치른다는 점을 고려하여 필기 10만 원과 실기 10만 원으로 설정. CLG는 초/중/고 학생 등의 정보보호(안)에 대한 관심과 리더러시를 높이고자 하는 목표를 가진 자격으로서 보편적으로 누구나 응시할 수 있도록 3만 원으로 설정

<표 2-43> 검정 수수료 설정 시 참고자료

구분		검정 수수료 현황
국가자격	정보보안기사	필기 18,800원, 실기 21,900원
	빅데이터분석기사	필기 17,800원, 실기 : 40,800원
	정보처리기사	필기 19,400원, 실기 22,600원
민간자격	개인정보관리사 (CPPG)	130,000원 [단체 15인 이상 20% 할인, 학생 50% 할인]
	블록체인관리사 (CBM)	1급·2급·3급 필기 150,000원, 1급·2급 실기 150,000원
	인터넷보안 전문가	1급·2급 필기 43,000원, 1급 실기 100,000원
	해킹보안전문가	2급·3급 필기 50,000원, 2급 실기 50,000원 주니어 25,000원(온라인검정)
	개인정보보호사	50,000원
	금융보안관리사(CFSE)	교육과정 80% 수료자(교육비 무료)
	정보보안관제사	1급 필기 55,000원, 실기 66,000원 2급 필기 44,000원, 필기 55,000원
	디지털포렌식전문가	1급 필기 100,000원, 실기 250,000원 2급 필기 60,000원, 실기 150,000원

○ 2종 민간자격의 출제기준은 다음과 같음.

## Cyber Risk Management Specialist (CRMS) 필기 출제기준

작성일 : 2023.11.22.

직무분야	정보통신(20) 정보기술(2001)	자격종목	사이버위험관리 전문가 Cyber Risk Management Specialist (CRMS)	적용기간	2024.1.1. ~ 2025.12.31.
직무내용	① 조직의 최고이사결정자들에게 조직의 위험 수준을 설명하고 이해시킬 수 있다. ② 조직의 정보자산을 식별하고 적절한 보안대책(통제방안)을 구현하여 조직이 감내할만한 수준으로 위험을 관리할 수 있다. ③ 경영진에게 보안 위험관리(분석·평가 포함)의 중요성을 설명하고 설득할 수 있다.				
필기 검정방법	객관식	문항수	80문항	시험시간	120분

□ 국가직무능력표준의 「정보보호관리·운영」 과 「개인정보보호」 에 해당하는 자격체계

o 20.정보통신 > 01.정보기술 > 06.정보보호 > 01.정보보호관리·운영, 07.개인정보보호

과목명	세부항목	개요
<b>I. 사이버 위험 관리 계획</b> : 조직의 정보보호·개인정보보호를 위한 위험 관리 계획의 필요성을 이해한다.		
	①사이버 위험 관리 범위	위험 관리에 필요한 경영 의사결정 방법론을 이해·적용한다.
	②사이버 위험 관리 정책	위험 관리에 필요한 전사적인 보안정책을 수립할 수 있다.
	③사이버 위험 관리 거버넌스	조직의 보안 위험 통제를 위한 보고체계를 파악한다.
<b>II. 사이버 위험 평가</b> : 조직의 정보자산과 위험·위협·취약점 등을 식별하고, 위험을 평가할 수 있다.		
	①정보자산 식별	조직의 정보자산 종류와 범위를 파악한다.
	②사이버 위험 평가방법	정보자산 도입, 구현, 운영 단계의 위험 평가 방법을 이해한다.
<b>III. 사이버 위험 완화</b> : 조직이 가지고 있는 위험을 최소화하거나 예방할 방안을 강구·조치할 수 있다		
	①보안대책 구현	정보자산 보안대책을 이해하고 개념적으로 구현 가능하다.
	②보안대책 인증	체계적인 보안대책 구현을 위한 인증/평가 제도를 이해한다.
	③사이버 위험 관리 컴플라이언스	조직의 보안 의사결정을 위한 규제사항을 이해·적용한다.

과목명	문제수	세부항목	세부내용
I. 사이버 위험 관리 계획 : 조직의 정보보호·개인정보보호를 위한 위험 관리 계획의 필요성을 이해한다.			
	30 (100점)	①사이버 위험 관리 범위 20%	위험 관리의 개념과 목적 위험·위협·취약성·보안대책 정의와 범주 합리적 보안 의사결정 방법과 절차 프로젝트 관리 기법과 커뮤니케이션 스킬
		②사이버 위험 관리 정책 30%	정보보호 정책 수립 시 포함사항 및 절차 위험 관리 절차 및 흐름 분석 위험 관리 계획서·절차서·흐름도 작성
		③사이버 위험 관리 거버넌스 50%	정보보호 조직과 CSO·CPO의 구성과 역할 보안사고 대응과 절차, 보고체계 정보보호·개인정보보호 교육
II. 사이버 위험 평가 : 조직의 정보자산과 위험·위협·취약점 등을 식별하고, 위험을 평가할 수 있다.			
	20 (100점)	①정보자산 식별 50%	정보자산의 종류와 범위 산업·조직(기관)별 정보자산 중요도 정보기술 아키텍처와 보안 아키텍처
		②사이버 위험 평가방법 50%	기술 경제성 평가 방법론 (개념적 이해) 프로젝트 위험 요인과 평가 방법론 (개념적 이해) 보안 위험 요인과 평가 방법론 (개념적 이해)
III. 사이버 위험 완화 : 조직이 가지고 있는 위험을 최소화하거나 예방할 방안을 강구·조치할 수 있다			
	30 (100점)	①보안대책 구현 52%	정보통신망 보안 (접근통제, 클라우드보안) 정보시스템 보안 (시스템보안 대응기술·솔루션) 데이터 보안 (DB보안기술·솔루션, 암호통제)
		②보안대책 인증 24%	ISMS-P 인증기준 정보보호 사전점검 항목 개인정보 영향평가 절차
		③사이버 위험 관리 컴플라이언스 24%	정보통신망 이용 촉진 및 정보보호 등에 관한 법률 개인정보 보호법 / 개인정보의 안전성 확보조치 기준 국가정보보안기본지침 이외 정보보호 관련 법규정
	80 (300점)		

(참고 1) CRMS 시험 준비를 위한 주요 참고자료는 ISMS-P 인증기준 안내서(2023.11.) 및 정보보호 관련 인증 제도 및 규정입니다.

과목명	세부항목	참고자료
I. 사이버 위험 관리 계획 : 조직의 정보보호·개인정보보호를 위한 위험 관리 계획의 필요성을 이해한다.		
	①사이버 위험 관리 범위	인증기준 1.2. 위험 관리-1.2.2 현황 및 흐름분석
	②사이버 위험 관리 정책	인증기준 1.2. 위험 관리-1.2.4 보호대책 선정 인증기준 1.3. 관리체계 운영
	③사이버 위험 관리 거버넌스	인증기준 1.1. 관리체계 기반 마련 인증기준 2.1. 정책, 조직, 자산 관리 인증기준 2.2. 인적 보안 인증기준 2.3. 외부자 보안
II. 사이버 위험 평가 : 조직의 정보자산과 위험·위협·취약점 등을 식별하고, 위험을 평가할 수 있다.		
	①정보자산 식별	인증기준 (1.2. 위험 관리-1.2.1 정보자산 식별)
	②사이버 위험 평가방법	인증기준 (1.2. 위험 관리-1.2.3 위험 평가) 정보보안기사 필기 교과목 (위험분석 및 평가)
III. 사이버 위험 완화 : 조직이 가지고 있는 위험을 최소화하거나 예방할 방안을 강구·조치할 수 있다		
	①보안대책 구현 [개념 수준]	ISMS-P 인증기준 2.4. 물리 보안 ISMS-P 인증기준 2.5. 인증 및 권한관리 ISMS-P 인증기준 2.6. 접근통제 ISMS-P 인증기준 2.7. 암호화 적용 ISMS-P 인증기준 2.8. 정보시스템 도입 및 개발 보안 ISMS-P 인증기준 2.9. 시스템 및 서비스 운영관리 ISMS-P 인증기준 2.10. 시스템 및 서비스 보안관리 ISMS-P 인증기준 2.11. 사고 예방 및 대응 ISMS-P 인증기준 2.12. 재해복구 정보보안기사 필기 (정보보호 대책 구현 및 사고대응)
	②보안대책 인증	ISMS-P 인증 제도 정보보호 사전점검 개인정보 영향평가
	③사이버 위험 관리 컴플라이언스	ISMS-P 인증기준 1.4. 관리체계 점검 및 개선 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 개인정보 보호법 [안전성확보조치 기준] 국가정보보안기본지침

(참고 2) CRMS 자격제도 준비를 위해 ISMS-P 인증기준 안내서 이외에, 대학 전공교재 중 「정보보안 관리론」에 해당하는 교재와 다음의 정부 발간의 가이드라인에 대한 기술 용어와 정보보안 관리 방법에 대한 개념적 수준의 이해가 필요합니다.

- ① 한국인터넷진흥원 (2004), 정보보호관리체계 위협관리 가이드
- ② 한국인터넷진흥원 (2010), 침해사고 분석 절차 안내서 (KISA 안내·해설 제2010-8호)
- ③ 한국인터넷진흥원 (2014), 악성코드 분석 연구보고서
- ④ 개인정보보호위원회, 한국인터넷진흥원 (2020), 개인정보 영향평가 수행안내서
- ⑤ 과학기술정보통신부, 개인정보보호위원회, 한국인터넷진흥원 (2020), 정보보호 및 개인정보보호 관리체계 인증 리플릿
- ⑥ 과학기술정보통신부, 한국인터넷진흥원 (2020), 정보보호 최고책임자 CISO 길라잡이 (기본편)
- ⑦ 개인정보보호위원회 (2020), 개인정보 보호 법령 및 지침·고시 해설  
[2023년 개인정보 보호법 개정으로 해설서도 개정 발표 예정]
- ⑧ 개인정보보호위원회, 한국인터넷진흥원 (2020), 개인정보의 안전성 확보조치 기준 해설서  
[2023년 개인정보 보호법 개정으로 해설서도 개정 발표 예정]
- ⑨ 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2023-6호)
- ⑩ 과학기술정보통신부, 한국인터넷진흥원 (2021), 주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드
- ⑪ 주요정보통신기반시설 취약점 분석·평가 기준 (과학기술정보통신부 고시 제2021-28호)
- ⑫ 과학기술정보통신부, 한국인터넷진흥원 (2021), 정보보호 최고책임자 지정·신고제도 안내서,
- ⑬ 개인정보보호위원회 (2021), 생체정보 보호 가이드라인
- ⑭ 개인정보보호위원회 (2021), 인공지능(AI) 개인정보보호 자율점검표
- ⑮ 과학기술정보통신부, 한국정보통신기술협회 (2022), 신뢰할 수 있는 인공지능 개발 안내서(안)
- ⑯ 한국인터넷진흥원 (2022), 정보보호 사전점검 해설서
- ⑰ 한국인터넷진흥원 (2022), 2022년 하반기 사이버 위협 동향 보고서
- ⑱ 개인정보보호위원회 (2022), 개인정보 처리방침 작성지침
- ⑲ 개인정보보호위원회 (2022), 가명정보 처리 가이드라인
- ⑳ 국가정보원 (2023), 국가 정보보안 기본지침
- ㉑ 과학기술정보통신부, 한국인터넷진흥원 (2023), 정보보호 공시 가이드라인
- ㉒ 과학기술정보통신부, 한국인터넷진흥원 (2023), 랜섬웨어 대응 가이드라인

# Cyber Risk Management Specialist (CRMS) 실기 출제기준

작성일 : 2023.11.22.

직무분야	정보통신(20) 정보기술(2001)	자격종목	사이버위험관리 전문가 Cyber Risk Management Specialist (CRMS)	적용기간	2024.1.1. ~ 2025.12.31.
직무내용	① 조직의 최고이사결정자들에게 조직의 위험 수준을 설명하고 이해시킬 수 있다. ② 조직의 정보자산을 식별하고 적절한 보안대책(통제방안)을 구현하여 조직이 감내할만한 수준으로 위험을 관리할 수 있다. ③ 경영진에게 보안 위험관리(분석/평가 포함)의 중요성을 설명하고 설득할 수 있다.				
실기 검정방법	필답형	문항수	5문항	시험시간	90분

과목명	주요항목	
I. 보호대책 구현  3(60점)	①사이버 위험 평가	의미 있는 위험평가에 필요한 위험의 모든 구성요소 (위험-위협-취약점-대책)를 결합하여 종합적으로 판단하는 방법을 이해하는가  실제 또는 발생 가능한 취약점을 식별할 수 있는 정도의 시스템 보안 측면의 특성을 결정하고, 이해하는가
	②보안대책 구현	식별된 위험을 삭제·감소·완화하는데 필요한 최적의 기술적 보안조치를 선택하고 구현 가능한가  복잡한 시나리오를 이해하고, 그의 해결을 위해 필요한 각기 다른 범주의 기술적 기법들을 결합하여 사용 가능한가
II. 보안 관리체계 운영  2(40점)	①사이버 위험 관리 컴플라이언스	생각할 수 있는 모든 위험(가정)을 명확하게 설명할 수 있는 능력과 그러한 위험을 제거할 수 있는 정보를 사용 가능한가  위험이 실현되었을 때 가져올 파장을 이해 가능한 비즈니스 용어로 설명 가능한가
	②사이버 위험 관리 거버넌스	위험과 보안의 개념을 조직의 수장들과 그들의 대변자들이 명확히 이해할 수 있도록 효과적으로 의사소통 가능한가  위험·위협 상황에 적합한 최적의 대책을 선택하고 그러한 대책의 경제성을 조직의 수장들과 그들의 대변자들에게 설득 가능한가

## Cyber Literacy Generalist (CLG) 필기 출제기준

작성일 : 2023.11.22.

직무분야	정보통신(20) 정보기술(2001)	자격종목	사이버보안 수학능력평가 Cyber Literacy Generalist (CLG)	적용기간	2024.1.1. ~ 2025.12.31.
검증목표	① 정보통신의 발전과 궤를 함께하는 정보보호 이슈와 기술을 이해할 수 있다. ② 지능정보 서비스 사용자로서 지켜야 하는 규칙들을 이해하고 적용할 수 있다. ③ 디지털 기술과 정보를 위한 안전한 컴퓨팅 환경을 이해할 수 있다.				
검증내용	① 정보보호 역사를 이해하고 정보보호의 필요성을 잘 인식하고 있는가 ② 지능정보사회를 살아가는데 필요한 기본적인 정보보호 기술을 알고 있는가 ③ 정보보호의 목표, 대상, 방법을 이해하고 적용할 수 있는가				
필기 검정방법	객관식	문항수	80문항	시험시간	2시간

과목명	세부항목	개요
I. 정보보호 역사 : 정보통신 발전 과정에서의 정보화의 진행 방향과 정보보호의 역할을 이해한다.		
	①정보통신의 발전과 정보보호	주요 통신 수단이 정보통신이 된 과정을 이해하고, 그 안에서 사회의 변화 방향과 정보보호의 역할을 이해한다.
	②지능정보기술과 정보보호	다양한 지능정보기술을 개념적으로 이해하고, 발생 가능한 정보보호 문제를 이해한다.
II. 정보보호 관리 : 정보보호의 목표 달성을 위해 필요한 관리 방법과 절차를 이해한다.		
	①정보보호의 목표	정보보호의 목표를 이해한다.
	②정보보호의 대상	보호대상의 종류와 정보자산으로서의 중요도를 이해한다.
	③정보보호의 방법	관리적 차원의 기본적인 정보보호 방법을 이해한다.
III. 정보보호 기술 : 정보보호 및 개인정보보호를 위해 필요한 기술의 개념과 구현 절차를 이해한다.		
	①네트워크와 정보보호	네트워크 보안 위협과 보안대책을 이해한다.
	②해킹과 정보보호	해킹의 종류와 보안대책을 이해한다.
IV. 정보보호 문화 : 지능정보기술 사회에서의 인터넷 문화와 보안윤리를 이해한다.		
	①사회적 이슈와 정보보호	경제·사회 전반의 활동에 정보통신기술이 내재됨에 따라 발생하는 사회적 이슈에서의 정보보호 문제를 이해한다.
	②지능정보기술과 보안윤리	인적보안 관리 차원의 보안윤리를 이해한다.

과목명	문제수	주요항목	세부내용
<b>I. 정보보호 역사 : 정보통신 발전 과정에서의 정보화의 진행 방향과 정보보호의 역할을 이해한다.</b>			
	10 (100점)	①정보통신의 발전과 정보보호 50%	통신 수단의 발전과 정보통신 정보보호 대상과 기술의 변천 디지털 전환 방향과 정보보호의 역할
		②지능정보기술과 정보보호 50%	인공지능·빅데이터 보안 융합산업(스마트제조, 스마트시티 등) 보안 개인정보 보호와 활용(마이데이터 등)
<b>II. 정보보호 관리 : 정보보호의 목표 달성을 위해 필요한 관리 방법과 절차를 이해한다.</b>			
	30 (300점)	①정보보호의 목표 33%	정보보호의 역할 기밀성, 무결성, 가용성
		②정보보호의 대상 33%	정보자산 네트워크 및 시스템 정보(개인정보 포함) 및 데이터
		③정보보호의 방법 33%	CISO·CPO 개념과 정보보호 교육 보안인식 제고
<b>III. 정보보호 기술 : 정보보호 및 개인정보보호를 위해 필요한 기술의 개념과 구현 절차를 이해한다.</b>			
	30 (300점)	①네트워크와 정보보호 50%	바이러스와 웜·멀웨어 개념 방화벽과 가상사설망 개념 디지털 포렌식과 보안 관제 개념 모의해킹 및 취약점 점검 프로세스 개념
		②해킹과 정보보호 50%	위험·위협·취약점·보안수칙(이용자) 시스템 해킹의 개념과 보안수칙(이용자) 네트워크 해킹의 개념과 보안수칙(이용자) 웹 해킹의 개념과 보안수칙(이용자)
<b>IV. 정보보호 문화 : 지능정보기술 사회에서의 인터넷 문화와 보안윤리를 이해한다.</b>			
	10 (100점)	①사회적 이슈와 정보보호 50%	Information Security와 Cyber Security 인터넷 공간의 확대와 사이버 범죄 소셜네트워킹의 발전과 사이버 폭력
		②지능정보기술과 보안윤리 50%	인공지능·빅데이터 발전의 윤리적 이슈 지능정보사회의 특성과 윤리 개인정보 보호와 활용의 윤리적 이슈
	80 (800점)		

- 2종 민간자격에 대해 등록을 위한 ‘민간자격관리·운영 규정’은 다음과 같음. 자격기본법 시행규칙 제2조 제2항의 사항을 담아, 자격의 종목·등급·직무내용에 관한 사항 등을 담아 작성함.

## 사이버위험관리전문가(Cyber Risk Management Specialist, CRMS) 자격 관리·운영 규정

제정: 2023년 11월 22일

### 제1장 총 칙

제1조(목적) 이 규정은 민간자격검정(이하 “검정”이라 한다.)의 업무를 엄정하고, 효율적으로 시행하기 위하여 필요한 사항에 대하여 규정함을 목적으로 한다.

제2조(용어의 정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. “시험위원”이라 함은 출제위원, 감수위원, 본부위원, 책임관리위원, 시설관리위원, 보조위원, 시험감독위원, 복도감독위원, 방송통제위원, 실기보조위원, 채점위원 및 기타 독찰위원을 말한다.
2. “답안지”라 함은 검정 시행종목 중 수작업에 의하여 채점되는 필기시험 답안지(주관식 시험문제지 포함) 및 실기시험 시행 시 순수 필답형으로 시행하는 종목의 답안지를 말한다.

제3조(적용대상) 이 규정은 검정을 시행하는 ICT자격본부 소속 직원과 검정 관련업무 종사자(시험위원 등) 및 기타 검정업무와 관련이 있는 자(수험자 등)에게 적용한다.

### 제2장 자격검정 시행조직

제4조(검정업무의 구분) ① ICT자격본부는 민간자격의 검정업무 전반을 주관·시행하며, 다음 각호의 업무를 수행한다.

1. 출제위원, 감독위원, 평가위원 위촉에 관한 사항
2. 시험의 과목선정, 출제, 시험, 감독, 채점 및 평가에 관한 사항
3. 시험시행 계획 수립 및 시행에 관한 사항

4. 합격자 확정에 관한 사항
5. 부정행위자 처리에 관한 사항
6. 합격자 관리 및 자격수첩 발급·관리에 관한 사항
7. 검정사업 일반회계 운영에 관한 사항
8. 기타 민간자격검정 업무와 관련된 사항

제5조(출제위원 등 선정 및 자격) ① 출제위원은 자격검정의 시험문제를 출제하며, 해당 분야에 전문가로 위촉한다. ② 감독위원은 필기 및 실기시험의 진행 및 감독 업무를 담당하며, ICT자격본부 내 팀장급 이상으로 위촉한다. ③ 평가위원은 평가 및 채점하며 해당 분야 전문가로 한다. ④ 출제위원, 감독위원, 평가위원 등에 위촉된 자에 대해서는 시험문제의 보안을 위해 소정의 서약서를 징구하여야 한다.

제6조(출제·감수위원 위촉 기준) 출제위원 또는 감수위원의 위촉기준은 다음 각호에 해당하는 자로 위촉한다.

1. 해당 종목 분야에서 10년 이상 산업체에 종사하는 자
2. 대학교 또는 전문대학에서 해당 기술 분야 전임강사 이상으로 재직하는 자
3. 해당 분야에 관한 학식(전공)과 경험이 풍부하여 자격이 있다고 인정되는 자

### 제3장 자격의 종목 및 검정

제7조(민간자격의 취득) 본 민간자격을 취득하고자 하는 자는 시험에 응시하여 합격하여야 한다.

제8조(자격종목 및 등급) 자격의 종목명은 사이버위험관리전문가(Cyber Risk Management Specialist, CRMS)이며, 단일 등급으로 한다.

제9조(자격소지자의 직무내용) ① 사이버위험관리전문가(Cyber Risk Management Specialist, CRMS) 자격증은 “조직의 정보자산을 식별하고 적절한 보안대책(통제 방안)을 구현하여 조직이 감내할만한 수준으로 위험을 관리하고, 경영진에게 보안 위험관리(분석·평가 포함)를 설명하고 설득할 수 있다”를 직무내용으로 한다.

② 등급별 직무내용은 다음과 같다. [※필수 기재사항]

자격명	등급	직무내용
사이버위험관리전문가 (Cyber Risk Management Specialist, CRMS)	단일	조직의 정보자산을 식별하고 적절한 보안대책(통제방안)을 구현하여 조직이 감내할만한 수준으로 위험을 관리하고, 경영진에게 보안 위험관리(분석·평가 포함)를 설명하고 설득할 수 있다.

제10조(검정의 기준) 검정의 기준은 다음과 같다. **[※필수 기재사항]**

자격명	등급	검정기준
사이버위험관리전문가 (Cyber Risk Management Specialist, CRMS)	단일	사이버위험관리 전문가로서 갖추어야 할 지식에 대한 검정과 실무에 적용할 수 있는 능력을 검정

제11조(검정방법 및 검정과목) ① 검정방법과 검정과목은 다음과 같다. **[※필수 기재사항]**

등급	검정방법	검정 과목(분야 또는 영역)
구분 없음	필기 3과목 80문항, 객관식 택일형	① 사이버 위험 관리 계획 ② 사이버 위험 평가 ③ 사이버 위험 완화
	실기 2과목 5문항, 필답형	① 보안대책 구현 ② 관리체계 운영

② 검정방법 및 검정과목별 문항수와 시험시간은 별표 1과 같다.

제12조(응시자격) 응시자격은 다음과 같다. **[※필수 기재사항]**

등급	응시자격
구분 없음	학사 이상 [학위증명서 또는 졸업예정증명서 제출 필요] 대학 졸업자 또는 졸업예정자 (전공 무관, 경력자의 경우 직무 분야 무관) 및 이에 상응하는 조건

제13조(검정의 일부 면제) ① 필기시험 합격 후 실기시험 불합격자 중에서, 차회 1회에 한정하여 필기시험을 면제한다.

제14조(합격결정 기준) ① 필기시험은 과목당 100점 만점 기준 40점 이상이며, 평균 점수가 60점 이상인 자를 합격자로 결정한다. ② 실기시험은 통합 100점 만점 기준 평균 점수가 60점 이상 득점자를 합격자로 결정한다. ③ 필기시험과 실기시험에 모두 합격한 자를 최종합격자로 결정한다.

## 제4장 수험원서

제15조(검정안내) ① ICT자격본부는 검정의 종목, 수험자격, 제출서류, 검정방법, 시험과목, 검정일시, 검정장소 및 수험자 유의사항 등을 포함한 검정안내서를 작성 배포할 수 있다. ② ICT자격본부의 모든 직원들은 수험자로부터 검정시행에 관한 문의가 있을 때, 이에 성실히 응답하여야 한다.

제16조(수험원서 등) ① 시험에 응시하고자 하는 자는 수험원서 및 응시자격 관련 서류를 제출하여야 한다. ② 수험원서 접수 시, 본인 사진을 필히 첨부하여야 한다. 사진 규격은 3×4cm이며, 파일 형식은 반드시 'jpg', 'gif', 'png' 중 한 가지이어야 하며, 파일 크기는 150KB를 넘지 않도록 한다.

제17조(원서접수) ① 원서접수, 검정수수료(이하 “수수료”라 한다) 수납업무는 인터넷 접수를 원칙으로 한다. ② 응시자격 증명이 필요한 경우 반드시 원본 서류를 우편 제출하여야 한다.

제18조(수험번호 부여) 원서접수에 따른 수험번호 부여는 지정된 수험번호 부여 규칙에 따라 부여하여야 한다.

제19조(검정수수료) ① 검정을 받고자 하는 자는 수수료를 납부하여야 한다. ② 검정을 받고자 하는 자가 이미 납부한 수수료는 과오납에 한하여 과오납 금액분만 환불하며, 이를 제외하고는 반환하지 아니한다. ③ 수수료에 대한 영수증은 별도 발급하지 않고, 수험표로 갈음한다. ④ 검정수수료는 필기와 실기로 구분하여 각각 소정의 수수료를 납부하여야 한다.

## 제5장 검정시행 준비

제20조(수험사항 공고 및 통지) ① ICT자격본부는 시행 자격종목, 시험일시, 수험자 지침물 등에 대해 온라인 수험원서 접수 시 게시 안내하여야 한다. ② 수험자 지침물 필수는 자격검정 수험표와 신분증(주민등록증 또는 운전면허증, 여권 등)이다.

제21조(시험장 준비) 시험장 책임자는 당해 종목 시행에 적합한 시설, 장비 등을 사전에 점검하여 시험 시행에 지장이 없도록 하여야 한다.

## 제6장 시험문제 출제 및 감수

제22조(시험문제의 개발, 보관, 관리 등) ① 시험문제의 유출을 방지하기 위하여 ICT 자격본부장은 시험문제의 인수, 보관, 관리 등에 대한 지휘·감독의 책임을 지고 보안 유지에 최선의 노력을 다하여야 한다. ② 시험문제는 인터넷 기반으로 개발하여 입력하고, 문제은행을 통하여 관리한다.

제23조(시험문제의 감수) ① 시험문제의 감수는 ICT자격본부가 운영하는 문제은행 시스템에서 수행한다. ② 시험문제 감수는 종목별 또는 과목별로 시행하되, 시험문제 출제 직후에 감수함을 원칙으로 하며, 필요에 따라 시험 직전에 재감수할 수 있다.

## 제7장 검정시험

제24조(수험자 교육) ① 감독위원은 배치된 시험실에 입장하여 수험자 유의사항, 시험시간, 시험진행 요령, 부정행위에 대한 처벌 및 답안지 작성요령 등을 주지시켜야 한다. ② 감독위원은 수험자에게 지정한 필기구, 시설·장비 또는 지급된 재료(공구) 이외의 사용을 금지시켜야 한다.

제25조(수험자 확인) ① 수험자는 입실 전 본인좌석을 반드시 확인 후 지정좌석에 착석하여야 한다. ② 감독위원은 시험에 있어서, 응시자 본인이 지참한 주민등록증 또는 기타 신분증과 수험표를 대조하여 수험자의 본인 여부를 확인하여야 한다. ③ 전산으로 진행됨에 따라, 안정적 운영을 위해 입실 후, 수험자는 감독위원 안내에 적극 협조하여야 한다.

제26조(시험감독 배치 및 시험 진행) ① 필기시험 및 실기시험의 감독위원 배치는 별표 2와 같이 배치한다. ② 최종 답안 제출 후 수정이 절대 불가하니, 수험자는 충분히 검토 후 최종 제출하여야 한다. ③ 필기시험은 전산으로 진행되므로 제출 후 본인 점수 확인 후, 수험자는 즉각 퇴실하여야 하며, 감독위원은 수험자의 퇴실을 안내하고 확인하여야 한다. ④ 실기시험은 필답고사로 진행되며, 채점은 사후에 진행됨을 원칙으로 하므로, 답안을 제출한 후에는 감독위원의 안내에 따라 퇴실하여야 한다.

제27조(시험시행결과보고) 책임관리위원은 시험 종료 후 그 결과를 ICT자격본부에

보고하여야 한다. 이 경우 시험진행 중 이상이 발생하였을 때에는 그 내용을 구체적으로 유선보고하고 차후 서면보고하여야 한다.

## 제8장 시험 채점 및 합격자 공고

제28조(필기시험의 채점) 필기시험의 채점은 전산 채점을 원칙으로 한다.

제29조(실기시험의 채점) ① 실기채점의 공정성, 효율성 제고 및 종목의 성격을 고려하여 감독 겸 채점위원을 위촉할 수 있다. ② 실기시험의 채점은 관계 전문가를 위촉하여 채점함을 원칙으로 한다.

제30조(최종 합격자 공고) ① 한국방송통신전파진흥원 원장은 검정 종료 후 30일 이내에 합격자를 공고하여야 한다.

제31조(자격증 교부) ① 합격자(예정자) 발표 후 10일 이내 우편으로 응시자격 증빙서류를 원본으로 제출하여야 한다. ② 최종합격자 중 응시자격 증빙서류를 제출한 자에 한하여, 자격수첩을 교부한다.

## 제9장 부정행위자 처리

제32조(부정행위자의 기준 등) ① 시험에 응시한 자가 그 검정에 관하여 부정행위를 한 때에는 당해 검정을 중지 또는 무효로 하고 3년간 응시 자격이 정지되며, 부정행위를 한 자라 함은 다음 각호의 1에 해당하는 자를 말한다.

1. 시험 중 시험과 관련된 대화를 하는 자
  2. 시험 중 시험문제 내용과 관련된 물건을 휴대하여 사용하거나 이를 주고받는 자
  3. 시험장 내외의 자로부터 도움을 받아 답안지를 작성한 자
  4. 사전에 시험문제를 알고 시험을 치른 자
  5. 다른 수험자와 성명 또는 수험번호를 바꾸어 제출한 자
  6. 대리시험을 치른 자 및 치르게 한 자
  7. 기타 부정 또는 불공정한 방법으로 시험을 치른 자
- ② 시험감독위원은 부정행위자를 적발한 때에는 즉시 수검행위를 중지시키고, 그 부정행위자로부터 그 사실을 확인하고 서명 또는 날인된 확인서를 받아야 하며, 그가 확인·날인 등을 거부할 시, 감독위원이 확인서를 작성하여 이에 날인 등의 거

부사실을 부기하고 입증자료를 첨부하여 서명날인한 후 책임관리위원회에 제출하여야 한다.

제33조(부정행위자 처리) ① 책임관리위원회는 시험감독위원으로부터 부정행위자 적발 보고를 받으면, 시험 종료 즉시 관계 증빙 등을 검토하여 부정행위자로 처리하고 수험자에게 응시제재 내용 등을 통보하는 한편 그 결과를 검정 종료 후 ICT자격본부에게 보고하여야 한다. ② 책임관리위원회는 부정행위 사실 인증을 판단하기가 극히 곤란한 사항은 관계 증빙서류를 첨부하여 ICT자격본부장에게 보고하여 그 결정에 따라 처리한다.

제34조(사후적발 처리) ① 수험자 간에 성명, 수험번호 등을 바꾸어 답안을 표시 제출한 때에는 양 당사자를 모두 부정행위자로 처리한다. ② 타인의 시험을 방해할 목적으로 수험번호 또는 성명 표시란에 타인의 수험번호 또는 성명을 기입한 사실이 입증된 때에는 행위자만을 부정행위자로 처리한다. ③ 책임관리위원회는 부정행위 사실이 사후에 적발한 경우, 적발한 자료를 증거로 하여 부정행위자로 처리하고, 해당 수험자에게 응시자격 제재내용을 통보하여야 한다.

제35조(시험장 질서유지 등) 감독위원회는 시험장 질서유지를 위하여 다음 각호의 1에 해당하는 행위를 하는 수험자에 대하여 시험을 중지시키고 퇴장시킬 수 있다.

1. 시험실을 소란하게 하거나, 타인의 수험행위를 방해하는 행위
2. 시험실(장) 내의 각종 시설, 장비 등을 파괴, 손괴, 오손하는 행위
3. 검정시설·장비 또는 공구사용법 미숙으로 기물손괴 또는 사고우려가 예상되는 행위
4. 기타 시험실의 질서유지를 위하여 퇴장시킬 필요가 있거나, 응시행위를 중지시킬 필요가 있다고 인정하는 행위

## 제10장 보칙

제36조(업무편람 작성, 비치) 검정업무 수행에 따른 세부적인 업무처리기준, 처리과정, 구비서류, 서식 등을 구분 명시한 민간자격검정 업무편람을 작성·비치하여 활용한다.

제37조(자격검정위원회 구성 등) ① 자격검정의 객관적이고 효율적인 운영을 위해 ICT자격본부 내에 ‘사이버위험관리전문가자격검정위원회(이하 “위원회”라 한다)’를

구성하고 이를 관리하기 위한 사무국을 둘 수 있다. ② 사무국은 자격검정의 시험 과목을 상시 점검하여 시의적절한 자격검정이 이루어질 수 있도록, 자격검정을 위한 문제은행의 최신화를 추진한다. ③ 위원회에 ‘사이버위험관리전문가자격검정위원회’의 장(이하 “위원장”이라 한다) 1인과 출제위원 3인, 감독위원 3인 및 평가위원 3인을 둘 수 있다. 다만, 출제위원과 평가위원은 겸임할 수 있다.

#### 부 칙

제1조(시행일) 이 규정은 제정한 날로부터 시행한다.

제2조(경과조치) 이 규정의 시행 이전에 시행된 사항에 관하여는 이 규정에 의하여 시행된 것으로 본다.

[별표 1] 과목별 시험 문항 수 및 시험시간표(제11조 관련)

구분	시험과목	문항 수 (배점)	세부항목	시험시간
필기	사이버 위험 관리 계획	30 (100점)	①사이버 위험 관리 범위 20%	40분
			②사이버 위험 관리 정책 30%	
			③사이버 위험 관리 거버넌스 50%	
	사이버 위험 평가	20 (100점)	①정보자산 식별 50%	40분
			②사이버 위험 평가방법 50%	
	사이버 위험 완화	30 (100점)	①보안대책 구현 52%	40분
			②보안대책 인증 24%	
③사이버 위험 관리 컴플라이언스 24%				
		80 (300점)		120분
실기	보호대책 구현	3 (60점)	①사이버 위험 평가	90분
			②보안대책 구현	
	관리체계 운영	2 (40점)	①사이버 위험 관리 컴플라이언스	
			②사이버 위험 관리 거버넌스	
		5 (100점)		

[별표 2] 감독위원 배치기준(제26조 관련)

구분	시험위원	위촉인원	비고
필기	정감독	1명 이상	시험실당
	부감독	1명 이상	시험실당
	관리위원	2명 이상	시험실당
	본부위원	1명 이상	시험장당
	본부보조위원	2명 이상	시험장당
	안내위원	2명 이상	시험장당
	복도감독위원	2명 이상	시험장당
실기	감독위원	2명 이상	종목당, 1일
	책임관리위원	1명 이상	시험장당, 1일
	관리위원	2명 이상	종목당, 1일
	진행위원	1명 이상	시험장당, 1일

# 사이버보안수학능력평가(Cyber Literacy Generalist, CLG) 자격 관리·운영 규정

제정: 2023년 11월 22일

## 제1장 총 칙

제1조(목적) 이 규정은 민간자격검정(이하 “검정”이라 한다.)의 업무를 엄정하고, 효율적으로 시행하기 위하여 필요한 사항에 대하여 규정함을 목적으로 한다.

제2조(용어의 정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. “시험위원”이라 함은 출제위원, 감수위원, 본부위원, 책임관리위원, 시설관리위원, 보조위원, 시험감독위원, 복도감독위원, 방송통제위원, 실기보조위원, 채점위원 및 기타 독찰위원을 말한다.

제3조(적용대상) 이 규정은 검정을 시행하는 ICT자격본부 소속 직원과 검정 관련업무 종사자 (시험위원 등) 및 기타 검정업무와 관련이 있는 자(수험자 등)에게 적용한다.

## 제2장 자격검정 시행조직

제4조(검정업무의 구분) ① ICT자격본부는 민간자격의 검정업무 전반을 주관·시행하며, 다음 각호의 업무를 수행한다.

1. 출제위원, 감독위원, 평가위원 위촉에 관한 사항
2. 시험의 과목선정, 출제, 시험, 감독, 채점 및 평가에 관한 사항
3. 시험시행 계획 수립 및 시행에 관한 사항
4. 합격자 확정에 관한 사항
5. 부정행위자 처리에 관한 사항
6. 합격자 관리 및 자격수첩 발급·관리에 관한 사항
7. 검정사업 일반회계 운영에 관한 사항
8. 기타 민간자격검정 업무와 관련된 사항

제5조(출제위원 등 선정 및 자격) ① 출제위원은 자격검정의 시험문제를 출제하며, 해당 분야에 전문가로 위촉한다. ② 감독위원은 필기 및 실기시험의 진행 및 감독

업무를 담당하며, ICT자격본부 내 팀장급 이상으로 위촉한다. ③ 평가위원은 평가 및 채점하며 해당 분야 전문가로 한다. ④ 출제위원, 감독위원, 평가위원 등에 위촉된 자에 대해서는 시험문제의 보안을 위해 소정의 서약서를 징구하여야 한다.

제6조(출제·감수위원 위촉 기준) 출제위원 또는 감수위원의 위촉기준은 다음 각호에 해당하는 자로 위촉한다.

1. 해당 종목 분야에서 10년 이상 산업체에 종사하는 자
2. 대학교 또는 전문대학에서 해당 기술 분야 전임강사 이상으로 재직하는 자
3. 해당 분야에 관한 학식(전공)과 경험이 풍부하여 자격이 있다고 인정되는 자

### 제3장 자격의 종목 및 검정

제7조(민간자격의 취득) 본 민간자격을 취득하고자 하는 자는 시험에 응시하여 합격하여야 한다.

제8조(자격종목 및 등급) 자격의 종목명은 사이버보안수학능력평가(Cyber Literacy Generalist, CLG)이며, 단일 등급으로 한다.

제9조(자격소지자의 직무내용) 사이버보안수학능력평가(Cyber Literacy Generalist, CLG) 자격증은 국가직무능력표준의 「정보보호관리·운영」과 「개인정보보호관리·운영」에 해당하는 지식 및 기술에 대한 기초소양을 측정한다.

② 등급별 직무내용은 다음과 같다. [※필수 기재사항]

자격명	등급	직무내용
사이버보안수학능력평가(Cyber Literacy Generalist, CLG)	단일	국가직무능력표준의 「정보보호관리·운영」과 「개인정보보호관리·운영」에 해당하는 지식 및 기술에 대한 기초소양(학습수준)을 측정한다.

제10조(검정의 기준) 검정의 기준은 다음과 같다. [※필수 기재사항]

자격명	등급	검정기준
사이버보안수학능력평가(Cyber Literacy Generalist, CLG)	단일	사이버 보안관리 분야로의 진학이나 취업을 고려하는 기술 및 지식 보유 수준을 검정

제11조(검정방법 및 검정과목) ① 검정방법과 검정과목은 다음과 같다. [※필수 기재사항]

등급	검정방법	검정 과목(분야 또는 영역)
구분 없음	필기 4과목 80문항, 객관식 택일형	① 정보보호 역사 ② 정보보호 관리 ③ 정보보호 기술 ④ 정보보호 문화
	실기 : 없음	

② 검정방법 및 검정과목별 문항수와 시험시간은 별표 1과 같다.

제12조(응시자격) 응시자격은 다음과 같다. [※필수 기재사항]

등급	응시자격
구분 없음	나이·학력·전공·실무경력 제한 없음

제13조(합격결정 기준) ① 합격 기준은 없으며, 응시자가 학습한 지식 및 기술 수준을 점수로 획득하여 확인하는 방식이다. 획득 점수에 따른 검증 결과 수준의 기준은 별표 3과 같다.

#### 제4장 수험원서

제14조(검정안내) ① ICT자격본부는 검정의 종목, 수험자격, 제출서류, 검정방법, 시험과목, 검정일시, 검정장소 및 수험자 유의사항 등을 포함한 검정안내서를 작성 배포할 수 있다. ② ICT자격본부의 모든 직원들은 수험자로부터 검정시행에 관한 문의가 있을 때, 이에 성실히 응답하여야 한다.

제15조(수험원서 등) ① 시험에 응시하고자 하는 자는 수험원서 및 응시자격 관련 서류를 제출하여야 한다. ② 수험원서 접수 시, 본인 사진을 필히 첨부하여야 한다. 사진 규격은 3×4cm이며, 파일 형식은 반드시 'jpg', 'gif', 'png' 중 한 가지이어야 하며, 파일 크기는 150KB를 넘지 않도록 한다.

제16조(원서접수) ① 원서접수, 검정수수료(이하 “수수료”라 한다) 수납업무는 인터넷 접수를 원칙으로 한다. ② 응시자격 증명이 필요한 경우 반드시 원본 서류를 우편 제출하여야 한다.

제17조(수험번호 부여) 원서접수에 따른 수험번호 부여는 지정된 수험번호 부여 규칙에 따라 부여하여야 한다.

제18조(검정수수료) ① 검정을 받고자 하는 자는 수수료를 납부하여야 한다. ② 검정을 받고자 하는 자가 이미 납부한 수수료는 과오납에 한하여 과오납 금액분만 환불하며, 이를 제외하고는 반환하지 아니한다. ③ 수수료에 대한 영수증은 별도 발급하지 않고, 수험표로 같음한다. ④ 검정수수료는 필기와 실기로 구분하여 각각 소정의 수수료를 납부하여야 한다.

## 제5장 검정시험 준비

제19조(수험사항 공고 및 통지) ① ICT자격본부는 시행 자격종목, 시험일시, 수험자 지침물 등에 대해 온라인 수험원서 접수 시 게시 안내하여야 한다. ② 수험자 지침물 필수는 자격검정 수험표와 신분증(주민등록증 또는 운전면허증, 여권 등)이다.

제21조(시험장 준비) 시험장 책임자는 당해 종목 시행에 적합한 시설, 장비 등을 사전에 점검하여 시험 시행에 지장이 없도록 하여야 한다.

## 제6장 시험문제 출제 및 감수

제20조(시험문제의 개발, 보관, 관리 등) ① 시험문제의 유출을 방지하기 위하여 ICT자격본부장은 시험문제의 인수, 보관, 관리 등에 대한 지휘·감독의 책임을 지고 보안 유지에 최선의 노력을 다하여야 한다. ② 시험문제는 인터넷 기반으로 개발하여 입력하고, 문제은행을 통하여 관리한다.

제21조(시험문제의 감수) ① 시험문제의 감수는 ICT자격본부가 운영하는 문제은행 시스템에서 수행한다. ② 시험문제 감수는 종목별 또는 과목별로 시행하되, 시험문제 출제 직후에 감수함을 원칙으로 하며, 필요에 따라 시험 직전에 재감수할 수 있다.

## 제7장 검정시험

제22조(수험자 교육) ① 감독위원은 배치된 시험실에 입장하여 수험자 유의사항, 시험시간, 시험진행 요령, 부정행위에 대한 처벌 및 답안지 작성요령 등을 주지시켜

야 한다. ② 감독위원은 수험자에게 지정한 필기구, 시설·장비 또는 지급된 재료(공구) 이외의 사용을 금지시켜야 한다.

제23조(수험자 확인) ① 수험자는 입실 전 본인좌석을 반드시 확인 후 지정좌석에 착석하여야 한다. ② 감독위원은 시험에 있어서, 응시자 본인이 지참한 주민등록증 또는 기타 신분증과 수험표를 대조하여 수험자의 본인 여부를 확인하여야 한다. ③ 전산으로 진행됨에 따라, 안정적 운영을 위해 입실 후, 수험자는 감독위원 안내에 적극 협조하여야 한다.

제24조(시험감독 배치 및 시험 진행) ① 필기시험 및 실기시험의 감독위원 배치는 별표 2와 같이 배치한다. ② 최종 답안 제출 후 수정이 절대 불가하니, 수험자는 충분히 검토 후 최종 제출하여야 한다. ③ 필기시험은 전산으로 진행되므로 제출 후 본인 점수 확인 후, 수험자는 즉각 퇴실하여야 하며, 감독위원은 수험자의 퇴실을 안내하고 확인하여야 한다.

제25조(시험시행결과보고) 책임관리위원은 시험 종료 후 그 결과를 한국방송통신전파진흥원 ICT자격본부에 보고하여야 한다. 이 경우 시험진행 중 이상이 발생하였을 때에는 그 내용을 구체적으로 유선보고하고 차후 서면보고하여야 한다.

## 제8장 시험 채점 및 합격자 공고

제26조(필기시험의 채점 및 점수 확인) ① 필기시험의 채점은 전산 채점을 원칙으로 한다. ② 시험 응시 종료 후, 응시자는 바로 획득한 점수를 확인할 수 있다.

제27조(자격증 교부) ① 시험 종료 후 10일 이내에, 응시자는 등록 시 선택한 자격증 교부 방식에 따라 자격증서를 받을 수 있다.

## 제9장 부정행위자 처리

제28조(부정행위자의 기준 등) ① 시험에 응시한 자가 그 검정에 관하여 부정행위를 한 때에는 당해 검정을 중지 또는 무효로 하고 3년간 응시 자격이 정지되며, 부정행위를 한 자라 함은 다음 각호의 1에 해당하는 자를 말한다.

1. 시험 중 시험과 관련된 대화를 하는 자
2. 시험 중 시험문제 내용과 관련된 물건을 휴대하여 사용하거나 이를 주고받는 자

3. 시험장 내외의 자료부터 도움을 받아 답안지를 작성한 자
4. 사전에 시험문제를 알고 시험을 치른 자
5. 다른 수험자와 성명 또는 수험번호를 바꾸어 제출한 자
6. 대리시험을 치른 자 및 치르게 한 자
7. 기타 부정 또는 불공정한 방법으로 시험을 치른 자

② 시험감독위원은 부정행위자를 적발한 때에는 즉시 수검행위를 중지시키고, 그 부정행위자로부터 그 사실을 확인하고 서명 또는 날인된 확인서를 받아야 하며, 그가 확인·날인 등을 거부할 시, 감독위원이 확인서를 작성하여 이에 날인 등의 거부사실을 부기하고 입증자료를 첨부하여 서명날인한 후 책임관리위원회에 제출하여야 한다.

제29조(부정행위자 처리) ① 책임관리위원은 시험감독위원으로부터 부정행위자 적발 보고를 받으면, 시험 종료 즉시 관계 증빙 등을 검토하여 부정행위자로 처리하고 수검자에게 응시제재 내용 등을 통보하는 한편 그 결과를 검정 종료 후 ICT자격본부에게 보고하여야 한다. ② 책임관리위원은 부정행위 사실 인증을 판단하기가 극히 곤란한 사항은 관계 증빙서류를 첨부하여 ICT자격본부장에게 보고하여 그 결정에 따라 처리한다.

제30조(사후적발 처리) ① 수험자 간에 성명, 수험번호 등을 바꾸어 답안을 표시 제출한 때에는 양 당사자를 모두 부정행위자로 처리한다. ② 타인의 시험을 방해할 목적으로 수험번호 또는 성명 표시란에 타인의 수험번호 또는 성명을 기입한 사실이 입증된 때에는 행위자만을 부정행위자로 처리한다. ③ 책임관리위원은 부정행위 사실이 사후에 적발한 경우, 적발한 자료를 증거로 하여 부정행위자로 처리하고, 해당 수험자에게 응시자격 제재내용을 통보하여야 한다.

제31조(시험장 질서유지 등) 감독위원은 시험장 질서유지를 위하여 다음 각호의 1에 해당하는 행위를 하는 수험자에 대하여 시험을 중지시키고 퇴장시킬 수 있다.

1. 시험실을 소란하게 하거나, 타인의 수험행위를 방해하는 행위
2. 시험실(장) 내의 각종 시설, 장비 등을 파괴, 손괴, 오손하는 행위
3. 검정시설·장비 또는 공구사용법 미숙으로 기물손괴 또는 사고우려가 예상되는 행위
4. 기타 시험실의 질서유지를 위하여 퇴장시킬 필요가 있거나, 응시행위를 중지시킬 필요가 있다고 인증하는 행위

## 제10장 보칙

제32조(업무편람 작성, 비치) 검정업무 수행에 따른 세부적인 업무처리기준, 처리과정, 구비서류, 서식 등을 구분 명시한 민간자격검정 업무편람을 작성·비치하여 활용한다.

제33조(자격검정위원회 구성 등) ① 자격검정의 객관적이고 효율적인 운영을 위해 ICT자격본부 내에 ‘사이버보안수학능력평가자격검정위원회(이하 “위원회”라 한다)’를 구성하고 이를 관리하기 위한 사무국을 둘 수 있다. ② 사무국은 자격검정의 시험과목을 상시 점검하여 시의적절한 자격검정이 이루어질 수 있도록, 자격검정을 위한 문제은행의 최신화를 추진한다. ③ 위원회에 ‘사이버보안수학능력평가자격검정위원회의 장(이하 “위원장”이라 한다)’ 1인과 출제위원 3인, 감독위원 3인 및 평가위원 3인을 둘 수 있다. 다만, 출제위원과 평가위원은 겸임할 수 있다.

## 부 칙

제1조(시행일) 이 규정은 제정한 날로부터 시행한다.

제2조(경과조치) 이 규정의 시행 이전에 시행된 사항에 관하여는 이 규정에 의하여 시행된 것으로 본다.

[별표 1] 과목별 시험 문항 수 및 시험시간표(제11조 관련)

구분	시험과목	문항 수 (배점)	세부항목	시험시간
필기	정보보호 역사	10 (100점)	정보통신의 발전과 정보보호 50%	60분
			지능정보기술과 정보보호 50%	
	정보보호 관리	30 (300점)	정보보호의 목표 33%	
			정보보호의 대상 33%	
			정보보호의 방법 33%	
	정보보호 기술	30 (300점)	네트워크와 정보보호 50%	
			해킹과 정보보호 50%	
	정보보호 문화	10 (100점)	사회적 이슈와 정보보호 50%	
			지능정보기술과 보안윤리 50%	
		80 (800점)		120분

[별표 2] 감독위원 배치기준(제24조 관련)

구분	시험위원	위촉인원	비고
필기	정감독	1명 이상	시험실당
	부감독	1명 이상	시험실당
	관리위원	2명 이상	시험실당
	본부위원	1명 이상	시험장당
	본부보조위원	2명 이상	시험장당
	안내위원	2명 이상	시험장당
	복도감독위원	2명 이상	시험장당
실기	감독위원	2명 이상	종목당, 1일
	책임관리위원	1명 이상	시험장당, 1일
	관리위원	2명 이상	종목당, 1일
	진행위원	1명 이상	시험장당, 1일

[별표 3] 획득 점수에 따른 검증 결과 수준의 기준

구분	내용	점수기준
수준 1	기초입문형 정보보호 기초 개념 학습이 필요한 수준	0점 ~ 149점
수준 2	기초도전형 정보보호 기본 개념을 이해하는 수준	150점 ~ 349점
수준 3	기본창의형 정보보호 기본 개념을 일상생활에 적용할 수 있는 수준	350점 ~ 499점
수준 4	문제통합형 정보보호 개념과 기술적 이슈를 통합적으로 이해하는 수준	500점 ~ 749점
수준 5	창의도전형 정보보호 지식과 기술을 모두 이해하고 응용할 수 있는 수준	750점 ~ 800점

## 제 4 절 민간자격 운영을 위한 시험문제 개발

○ CRMS와 CLG 각 검정의 시행을 위해 1회분 80문항의 5배수 출제

- CRMS 필기 : 정보보호를 전공한 석사 이상의 정보보호 관리(컨설팅) 업무에 종사중인 실무 인력으로 출제위원 구성
- CRMS 실기 : 정보보호 업무경력 10년 이상의 관리자급 인력으로 출제위원 구성 (정보보호 유관자격 검정 및 출제 경력 보유)
- CLG 필기 : 정보보호를 전공한 석사 이상의 정보보호 관리(컨설팅) 업무에 종사중인 실무인력으로 출제위원 구성

○ 출제위원 대상으로 출제기준 설명 → 의견 수렴하여 수정 → 출제기준 배포 → 출제

- 23년 8월 말부터 10월 중순까지 진행

		※ 관리번호	
종 목		난이도	하
과목명	개인정보 보호 원칙	문항번호	1

[문 제] 다음은 개인정보처리자가 신규 서비스를 기획하면서 준수해야 할 개인정보 보호 원칙을 근거로 해서 법적 위험을 고려해야 할 사항에 대한 설명이다. 빈칸에 알맞은 용어를 작성하시오.

① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 ( A ) 의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 ( B ) 이 보장되도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 제30조에 따른 ( C ) 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람 청구권 등 정보주체의 권리를 보장하여야 한다.

⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 ( D ) 처리가 가능한 경우에는 ( D )에 의하여, ( D ) 처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.

⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

( A ) :  
( B ) :  
( C ) :  
( D ) :

평가 목표	개인정보보호 원칙을 이해하고 원칙에 따른 위험을 분석할 수 있는 것에 대해 알아본다.
정답	정답 ( A ) : 최소한 ( B ) : 최신성 ( C ) : 개인정보 처리방침 ( D ) : 익명
배점	각 항목당 5점, 총20점 정확한 단어가 포함된 경우에만 정답으로 처리
참고자료	「개인정보 보호법」 제33조(개인정보 보호 원칙)
정답해설	① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다. ② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다. ③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다. ④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다. ⑤ 개인정보처리자는 제30조에 따른 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다. ⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다. ⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다. ⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

<그림 2-3> 회수한 출제문제 예시

○ 출제문제 회수하여, 검수

- CRMS 필기 : 정보보호 업무경력 10년 이상의 관리자급 인력 및 교수진 검수
- CRMS 실기 : 내부 연구진(정보보호 전공과정 운영 10년 이상의 교수) 검수
- CLG 필기 : 내부 연구진 검수

	A	B	C	D	E
1	코드	과목명	세부항목	문제번호	검토의견
2	CRMS-I-①-01	I. 위험 관리 계획	①	1	보기 3번 현업 → 업무담당자들의
3	CRMS-I-①-02	I. 위험 관리 계획	①	2	보기 4번 자산의 위협에 관한..
4	CRMS-I-①-05	I. 위험 관리 계획	①	5	4번/5번 문제 유사성
5	CRMS-I-①-08	I. 위험 관리 계획	①	8	난이도 하
6	CRMS-I-①-09	I. 위험 관리 계획	①	9	유사성
7	CRMS-I-①-10	I. 위험 관리 계획	①	10	난도도 중
8	CRMS-I-①-11	I. 위험 관리 계획	①	11	지문 3 번 4번 약간 중복 / 수정
9	CRMS-I-①-16	I. 위험 관리 계획	①	16	난이도 중
10	CRMS-I-①-28	I. 위험 관리 계획	①	28	띄어쓰기
11	CRMS-I-②-03	I. 위험 관리 계획	②	3	문제 수정
12	CRMS-I-②-04	I. 위험 관리 계획	②	4	보기 4번 퇴직자의 개인정보 파기 등
13	CRMS-I-②-08	I. 위험 관리 계획	②	8	난이도 하
14	CRMS-I-②-10	I. 위험 관리 계획	②	10	난이도 하
15	CRMS-I-②-12	I. 위험 관리 계획	②	12	난이도 하

<그림 2-4> 회수한 검수의견서 예시

○ 오탈자, 난이도, 물음방식, 문제보기기호, 띄어쓰기 등 일괄 교정

- 난이도는 검수/검토 의견이 합치되지 않는 경우, 출제자가 제시한 난이도를 우선 기준으로 함

## 제 3 장 공인민간자격 활성화 방안

### 제 1 절 활성화 방안

- 신규 자격제도의 안정화를 위해 초기 응시 자격기준을 광범위하게 잡고, 정보보호 전공자가 아니더라도 응시할 수 있도록 오픈

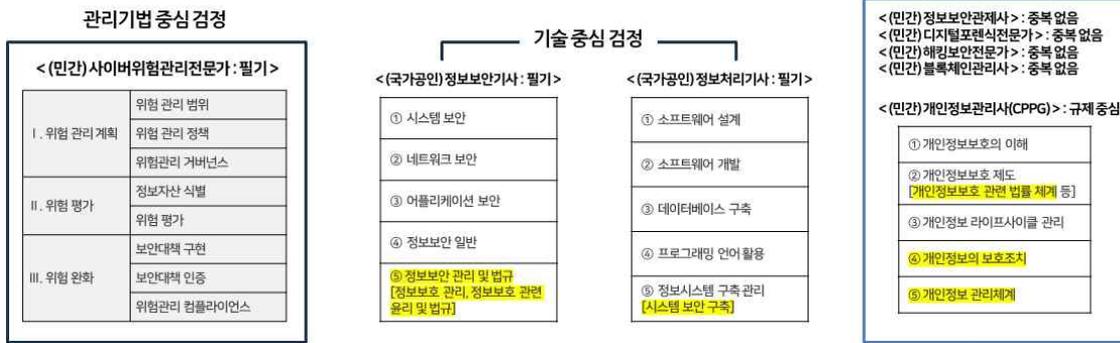


<그림 3-1> 공인민간자격 활성화 방안

- 응시요건 제한 최소화
  - 자격의 질 관리의 영향을 미치지 않는 범위 내에서 반드시 필요한 사항만을 응시 요건으로 제한
  - CRMS 자격의 경우 응시 자격은 학력 제한만 둠(4년제 졸업(예정) 이상)
  - CLG는 응시 자격에 별도 제한 없음
- 부분 합격제도 도입
  - 현재 국가공인 민간자격의 경우 대부분 종목이 검정 과목을 일시에 합격해야만 자격 부여가 가능
  - CRMS 자격의 경우 자격 취득에 필요한 지식 수준 및 학습 시간이 타 민간자격에 비해 높다고 볼 수 있으므로 자격 취득 기회의 확대를 위한 부분 합격제도 도입을 검토

○ Cyber Risk Management Specialist (CRMS)

- (교두보 역할을 하는 자격증으로 홍보) 정보보호 관리 전문가로서의 커리어패스를 만들고자 하는 인력을 대상으로, “CRMS → 정보보안(산업)기사 → ISMS-P 인증심사원”의 경로를 시작할 수 있다는 점과 기술 중심이 아닌 관리기법 중심의 새로운 검정임을 홍보 <그림 3-2>



<그림 3-2> CRMS와 다른 자격제도와의 차별성

- (정보보호학회 네트워크 활용한 홍보) 한국정보보호학회 홍보 채널을 통해 전국 정보보호 학회 교수들에게 홍보하고, 정보보호산업협회 등을 통해 산업체 전문 인력들에게 전문자격증으로 홍보

○ Cyber Literacy Generalist (CLG)

- (특성화고 재학생/졸업생에 대한 홍보 강화) 특성화고 담당 교사들에게 시험안내서 발송 등을 통해 자격 제도를 홍보하고, 보다 많은 학생/졸업자들이 응시할 수 있도록 주기적인 홍보물 발송
- (전문대학 재학생에 대한 홍보 강화) 전문대학 정보보안 교수진에게 시험안내서 발송 등을 통해 자격 제도 관련 주기적인 홍보물 발송
- (정보보안 교양과목 담당교수들에게 홍보 강화) 일반대학의 정보보안 관련 교양과목 담당 교수진들에게 자격증 시험안내서 발송 등을 비전공자 학생들도 정보보안 리터러시역량을 간접적으로 입증할 수 있는 기회 제공

## 제 2 절 공청회

- 2023년 11월 16일 신규 민간자격 2종에 대해 공청회를 개최하여, 각계각층의 의견을 청취하고, 전문가들의 토론을 진행함
- 연구진이 신규 민간보안자격 설명 <그림 3-3>



<그림 3-3> 공청회 - 연구진 발제

- 연구진 발제 이어, 토론 및 질의응답 진행하였으며 <그림 3-4>, 주요 의견은 다음과 같음
  - 자격증이 인력의 숙련도를 평가하는 도구가 되지는 못하지만, 현장에서 분명 수요는 있음
  - 정보보안 기사가 너무 난이도가 높고, 현업에서 실제 활용하는데 한계가 있음
  - 정보보안 기사는 기술사급으로 격상하여 품질을 유지하고, CRMS를 정보보안 기사를 대체 하되 난이도는 일반적이면 유리할 것임(정보보안 기능사 정도로 자리해도 좋을 듯함)

- 정보보호 이슈가 기업 입장에서 기술 중심이 아닌 관리 중심으로 넘어가고 있는 것은 트렌드임. 신규 자격제도가 이에 부합하는 것으로 보임
- 학교 입장에서 학생들의 학습 수준을 평가할 수 있는 기준이 될 수 있기에, 경력 개발을 위한 로드맵 수립 시에 학생들에게 좋은 마일스톤 역할을 할 것으로 기대
- 운영상의 안정성 확보가 무엇보다도 중요할 것(난이도와 출제범위의 일관성 유지 등)



<그림 3-4> 공청회 - 토론 및 질의응답

○ 공청회 결과 반영 사항

- 공청회를 통해 정보보호 분야의 2개의 민간 자격제도 신설의 필요성에 대해 공감대를 형성하고, 현재 과제를 통해 개발한 자격제도의 현실적인 운영을 위해 필요한 사항의 의견을 청취하였으며, 대부분 ‘안정적인 운영’을 위해 노력해 달라는 의견이었음
- CRMS의 경우 직접 직무에 투입할 인력을 배출하는데 필요한 자격이라는 점에서, 국가직무능력표준(NCS)과의 연계가 필요하다는 의견이 있어, 연계표를 최종보고서에 추가 작성 (pp.47-49)

## < 토론 및 질의응답 회의록 >

2023. 11. 16. 목

### (1) 토론자 의견

#### ○ 한국직업능력연구원 자격센터 센터장

- 기초/초급 수준의 범용 능력을 보유한 정보보호 인력이 중요하다고 생각
- 일을 하는데 사람의 지식이나 기술이나 소양 정도를 일정한 기준과 절차에 따라 평가해서 인정하는 것을 자격이라고 정의(자격기본법(1997년 제정))
- 민간자격은 국가자격에 비해 유연하게 설계 가능 (국자가격과 상충하지 않는다는 조건). 유연하고 신속한 기술 대응을 위해서는 민간자격으로 운영이 타당
- 민간자격 등록 업무를 직능연 자격센터에서 함. 민간자격 신설 시 : (1) 신설의 당위성 (수요가 있을 것이나, 산업/인력/교육훈련 분석을 통해 응시자 수요 규모를 면밀히 분석 필요), (2) 자격의 내용(직무분석 절차에 따라서 검정과목 도출을 하게 됨. 이 절차가 있어야 함. 현장의 어떤 수요에 대응할 것인지. NCS와의 연계 필요), (3) 자격의 활용성(자격을 취득한 사람이 시장에서 역량을 인정받을 수 있는 수단이 되도록. 가장 좋은 것은 법적으로 우대해 주는 것 이지만 민간자격은 어려운 부분임. 하지만, 검토는 필요) (4) 문제출제 및 운영은 누가 맡을지 (공신력 확보 부분)에 대한 현실적인 검토가 필요

#### ○ 한국방송통신전파진흥원 ICT자격본부 본부장

- KCA가 국가기술자격 운영을 맡은 지 10년 정도 됨. 1991년부터 전파법에 의한 무선 쪽 자격 검정에 대한 노하우 및 경험을 보유하고 있음. 정보보안기사는 2021년부터 해서 경험이 적음. 효율성 측면에서 KCA로 넘어온 것으로 생각하며, 정보보안기사를 운영하면서, 정보보호 분야에 대한 민간자격 발굴의 필요성을 느끼고 있음. 현 정부의 사이버보안 10만 인재 양성 등 글로벌 사이버 위협에의 대응 등을 위해 필요한 자격 신설 업무라고 생각
- 지능정보사회로의 진입에 있어 디지털 기술, 정보보호 기술 등이 활용되고 있는데, 이에 대한 기본적인 개념을 파악하고 있다면 일반인들조차도 쓸모가 있는 자격이 될 것으로 기대
- 코비드19로 디지털 전환이 가속화. 교육제도/자격검정 제도 자체가 디지털로 완전 전환 (CBT). 효율성이 좋아지지만, 정보시스템 파괴/침해 시 문제 되지 않나, 이에 대한 대응을 위해서라도 관리 측면의 정보보호 지식 확산은 필요하다고 생각하며 이를 뒷받침해 줄 수

- 있는 자격이 되지 않을까 기대(정보보안 관리에 대한 폭넓은 이해의 필요성을 강조하므로)
- 가능하다면 민간자격으로 운영 후 장기적으로 국가자격으로 만들기를 희망. 정보보안기사/산업기사 검정 시행 중인데, 기능사는 없음. 기능사와 연계할 수 있는 부분도 있을 것
- 자격 활성화를 위해서는 우대조건이 필수인데(취업 시 가점, 학점 취득에 도움이 된다던가), 법적 우대 조건 등을 부처와 협의해 보겠음
- 기존 자격과의 차별성(기술 vs 관리)을 강조하면, 시장의 수요는 충분할 것이라고 생각

○ 한국인터넷진흥원 미래정책연구실 실장

- 정보보호 역량 강화 및 사고대응을 주로 하니, 자격의 내용에 대해 코멘트하겠음
- 정보보호 분야는 규제 준수 활동에 대해 강조하는 활동으로 변화하고 있음. 경제사회 활동에 커다란 영향을 미치는 대형 사고가 발생해 온 탓 (대형 기간사업자의 랜섬웨어 감염으로 국가 통제 실패 등과 경제 손실)
- 사이버 위협을 어떻게 경제적인 가치로 환산하고 대응할 거냐. 즉, 사이버 리스크를 다루는 자격제도의 신설은 정보보호 영역을 기술 중심에서 관리 중심으로 확대하는 데 도움이 될 것임
- 자격의 내용은 실무적으로 고려해야 할 것이 있음 : 실무에서 다루는 사이버 위협을 공유하는 업무에서 사이버 위협은 (1) 기술적 (2) 관리적 (3) 전략적 관점에서 다름. 강조하고 싶은 것은 전략적 관점의 것. CEO/CSO/CIO들이 사이버보안 동향을 파악하고 조직에 녹여 넣는 의사결정을 하는데 필요한 내용을 예상하고 조직이 어떻게 움직여야 하는지 방향을 잡는 것이 이에 해당. 민간과 협력해 보니, 기술에 포커스 맞춰왔는데 최근에는 전략적/관리적 공유나 협력이 강조되고 있어, 민간 자격제도의 개설 방향은 맞는 것으로 생각함
- 이해관계자들이 기업의 사고에 대해 알권리 있음. 이해에 반하는 자산 손실에 해당하기 때문. 2023년 8월 SEC(미국증권거래위원회)는 미국의 사이버보안 disclosure 실시 발표 (거버넌스 (이사회에 보고했는지), 위협관리 및 전략(투자자가 이해할 수 있도록 쉽게 작성할 것. 조직 전체의 위협관리 프로세스와 유기적으로 연계되도록 할 것), 사이버사고 보고). 이 사례만 보아도, 보안의 중심이 '관리' 쪽으로 넘어가는 것은 시대적 흐름이라고 할 수 있음
- 국내 자격체계 대부분 보수교육을 안 하고 있는데, ISMS-P 같은 경우는 계속 보수교육을 하므로 그로 인한 혜택이 또 있음 (자격 취득 후 관리 및 연속성 확보, 정보보호 기술은 최신성 확보 등)

○ 한국정보보호산업협회 정보보호교육원 부원장

- 정보보호, 블록체인, 개인정보보호 NCS 개발 중
- 개인정보보호 분야 세분류 진행 중 (정보보호와 완전히 분리하여 별도 세분류로)
- 민간 자격제도 개발 시, NCS와 연계해야 할 것임
- 정보보안기사 합격률 1.9%는 심각. 정보처리기사는 30%
- 산업기사는 노동부/과기정통부와 협의, 과정평가형으로 진행 중이기에 합격률 30% 유지
- 정보보안기사도 과정평가형으로 가면 합격률 올릴 수도 있지 않을까 생각
- 정보보안기사 최종합격률 1.9%는 기술사 수준 아닌가, 아예 기술사로 올리고 정보보안기사 재설계가 필요한 것이 아닐지 생각
- 보안관계지정업체, 정보보호서비스지정업체 등은 정보보안기사, 4년제 졸업자 등이어야 초급 인력으로 봄. 따라서, 응시자격에 학력제한 필요하다고 생각 [연구진 의견 - CRMS 4년제 졸업자 이상을 응시조건으로 설정한 바 있음]
- CPPG-f라는 자격제도가 있음. 관심 유도 목적. 인터넷으로 실시
- 신규로 제안한 CLG 자격은 인식제고 차원으로 쉽게 접근해서 쉽게 보도록 한다면 (응시 자격 폭넓게 하는 방향이 매우 맞다고 생각) 목적을 달성할 수 있을 것이라고 생각

○ 단국대학교 교수 - 학생/교수/출제자 입장에서 얘기하겠음

- 사이버보안에 대한 관심이 증가. 학생의 관심도 높고, 기업의 니즈도 높은 편임
- 민간 자격증 제도 신설은 매우 시의적절하다고 생각
- 자격의 실효성/전문성/실무와의연계/운영주체의신뢰성 모두 중요. 평가체계(자격운영기관의 안정성)이 제일 중요하다고 생각. 운영전략 수립해서 흔들리지 말고 가야 함. 어떤 것을 공부해야 하는지 가이드하기도 함
- 자격은 이 직무에의 진입자격을 통제하는 역할을 하기도 함
- 시장은 인력에 대한 수요 높지만, 특정 자격을 획득하는 것이 너무 어렵다면, 이 자격이 제대로 역할하고 있는지 판단할 필요가 있음
- 내용적 측면/신뢰성 확보 측면에서 고민을 많이 한 신규 자격이라고 생각함
- 학생들이 시장에 진입하기 전에 나의 실력을 확인할 수 있는 교두보 역할을 할 수 있는 자격이 생긴다는 것은 고무적인 일이라고 생각
- 사후적인 대응을 많이 담고 있다는 점에서 기업 입장에서도 좋을 것 같음
- 평가체계 완성 시 안정성 확보에만 더욱 고민해 주시기를 바람(운영상의 안정성)

- 위험관리에 대한 공통적인 consensus 형성이 필요. 이 용어 자체가 매우 어려울 수 있음. 출제자의 출제의도가 잘못 발현될 수 있음. 과목명을 좀 더 clear하게 정의하면 좋겠음
- CLG는 과목1과 과목4가 문항 수가 적는데, 인식제고 역할을 하다보니 그런 것으로 생각. 차차 문항 수 밸런스를 맞추어 나가면 좋을 것으로 생각함
- 자격증 시험문제 출제할 때, 응시자를 생각하게 됨. 응시자가 준비 잘 해서 잘 따가도록 하려면, 운영체제의 안정성(중간에 난이도를 확 튼다든지 하지 않아야 함) 확보 매우 중요하다고 생각. 자격증 취득 자체가 목적이 아니라, 시장에 진입하고자 하는 마음을 갖도록 하는 역할도 좋을 것

## (2) 일반 청중의 질문 및 의견

### ○ 두두아이티

- CLG 의도 충분히 이해
- CRMS의 경우, 정보보안기사는 따기는 힘들지만 사용성은 건요하지 않음. ISMS-P는 일종의 라이선스 같은 역할을 하므로 활성화될 수밖에 없음. 최근에는 정보처리기사는 또 어느 정도 (소프트웨어 사업 투입 인력으로 조건으로 들어가므로) 의미가 있음. 그런데, 상주 투입인력에 정보보안기사는 쓸모가 없음. 따기는 힘들도 사용성은 낮음. CRMS는 그런 효과성이 더 떨어지지 않나 생각함
- [연구진 답변] 고민하는 부분임. 소프트웨어 등급이 처리기사만 있음 됨. 정보보안기사는 고려하지 않음. 애매한 부분이 있는데, 시행규칙 등에 넣어서 활성화시켜야 함. 우리가 사용처를 확대하고 넓혀 나가야 하는 것이지, 우리가 잘못된 것이고 노력해야 하는 부분이라고 생각. CRMS를 만들면 소프트웨어 인력 투입 등까지 넣는 작업은 반드시 필요하다고 생각

### ○ 해양경찰청 정보보안담당관

- 응시자 입장에서/공공기관 정보보안담당자/정보보호서비스 위탁운영자 입장에서 질문
- 정보보안기사 자체는 폐쇄적인 운영(출제기준, 출제 후 문제 open 등)이라는 비난을 받고 있음. 응시자 커뮤니티에서 정보보안기사에 대한 불만이 매우 높음. 응시자들과 소통할 수 있는 체계/질문 등을 활용해서 정보보안기사 합격률 높이거나 관리방안 수정 필요
- 산업기사와 기사 사이의 난이도 필요하지 않나. 기사는 기술사로 바꾸던지.
- 초급자/중급자/고급자 구분해 보면 정보보안기사 보유 여부로 실력을 판단하지는 않음. 실무에서는 gap이 거의 없음 [보통 관제부터 시작하는데]

- 실무에 맞는 자격이 필요함. 보안관제는 관리적인 역량이 매우 필요한데, 정보보안기사는 커버하지 못함. 침해사고 대응, 로그분석 등을 통해 원인 분석하는 부분은 고급역량. 잘 할 수 있는 인력 거의 없음. 이들의 전문성을 요할 수 있는 자격증 필요
- 보안 쪽 인력 이슈 있음 : 문턱 높는데, 급여는 작음. 우수인력 확보/유지 어려움
- 민간자격 만들 때도 응시자/기업 의견 수렴할 수 있는 창구 만들 수 있기를 바람
- [토론진행자 의견] 4학년 학생들이 정보보안기사 실기에서 다 떨어짐 (실무경험이 없어서). 이들을 위한 현실적인 자격이 필요하다고 생각
- [KCA 본부장 의견] 합격률은 많이 올랐음. 초기에 자격 품질을 잡으려고 했던 시도가 아니었을까 생각함. 시험문제 PBT와 CBT로 병행하다가 (PBT는 문제 공개했음) 내년부터는 CBT로 전체 전환. 문제 공개하기 어려움(문제를 엄청난 수로 만들어야 공개가 가능하기 때문에. 관리도 어려움. CBT는 열흘 이상 보기 때문에)

○ 한국방송통신전파진흥원 검정업무 이전 담당자

- 정보보안을 필드에서 하다보니, 기사에 대한 요구사항/합격률에 대한 요구가 있음
- 민간자격은 이론적인 사항을 평가(기술적인 평가보다는) 한다고 생각. 학교 교수님들이 보시기에 학생들 대상 홍보/인큐베이팅하는 측면도 있음. 자격으로만 끝나는 것이 아닌, 수업이나 보수교육과 접목이 가능할지 궁금
- ICT 자격 전문기관이다보니, 정보보호는 약한 부분이 있음. 학회나 협단체에서 교육을 함께 할 수 있을지 궁금
- [KISIA 부원장 의견] 보안기사도 과정평가형 자격제도로 넘어와야 함 (산업기사는 넘어옴). 교육을 하고 내/외부 평가를 통해 자격을 부여하는 것임. 보안기사도 과정평가형으로 넘어온다면 가능해 질 것. 교육기관은 산업부 등이 지정하게 되는 과정이 있음. 이런 경우 합격률 높일 수 있음. 완벽히 출제기준을 NCS 기준으로 맞춰야 함. 그러면 출제기준도 공개될 수 있음 (문제는 공개할 수 없다 하더라도)
- [단국대 교수 의견] 학교 입장에서는 자격에 대한 활용을 설명할 수 없으면 학생의 신뢰를 얻기 어려움. 업계에서 자격의 활용에 대해 같이 고민하면 좋은데, 아니라면 오히려 학생들의 신뢰도를 확 떨어트려서 자격제도에 대한 관심 자체를 무너트릴 수 있는 위험 있음
- [연구진 답변] 출제위원들도 실제 업무(정보보안 관리)를 하는 분들에게 위탁, 보안 관리 실무에서 고민하는 문제나 고민할 때 필요한 개념을 중심으로 출제. CRMS 특히 NCS 기반으로 옮기는 것, 보수교육/학과 중심으로 하는 문제는 세세하게 고민 필요