

The logo for PECB, featuring the letters 'PECB' in a bold, white, sans-serif font. The letters are slightly spaced out, and the 'P' and 'C' have a unique, stylized design with a small gap in the middle of each letter.

PECB

BEYOND RECOGNITION

A photograph of two business professionals, a woman in a dark suit and a man in a light suit, standing in a modern office hallway. They are looking at a tablet together. The background shows large glass windows and a clean, minimalist interior.

# ISO/IEC 27001 LEAD AUDITOR

## 수강생 핸드북

## 목차

---

<b>제 1 장: 서론</b> .....	<b>4</b>
PECB 윤리강령(Code of Ethics) .....	7
ISO/IEC 27001 선임심사원 소개 .....	9
<b>제 2 장: 시험 준비, 규칙 및 정책</b> .....	<b>10</b>
시험준비 및 일정 등록 .....	10
역량 영역 .....	11
시험 응시 .....	21
시험 보안 정책 .....	25
시험 결과 .....	26
시험 재응시 정책 .....	26
<b>제 3 장: 인증 프로세스 및 요구사항</b> .....	<b>28</b>
PECB ISO/ IEC 27001 자격 증명 .....	28
자격인증 신청 .....	29
실무 경력 .....	29
프로페셔널의 추천(Professional References) .....	30
ISMS 심사 경력 .....	30
자격인증 신청 검토 .....	30
<b>제 4 장: 자격인증 정책</b> .....	<b>31</b>
자격인증 거부 .....	31
자격인증 상태 옵션 .....	31
자격인증 업그레이드 및 다운그레이드 .....	32
자격인증 갱신 .....	33
자격인증 신청기간 만료 .....	33
민원 및 항의 정책 .....	33
<b>제 5 장: 일반정책</b> .....	<b>34</b>
기타 인증기관이 공인하는 시험 및 자격인증 .....	34

# PECB

차별금지 및 특수여건.....	34
행동 정책 .....	34
환불 정책 .....	35

## 제 1 장: 서론

---

### PECB 소개

PECB 는 다양한 분야에서 개인에 대한 교육 , 자격인증 및 자격증 프로그램을 제공하는 인증기관입니다.

전세계 150 여 개국에 진출하여 국제적으로 인정받는 표준에 따라 가치 있는 평가, 인증 및 자격증 프로그램을 제공함으로써 전문가들이 다양한 전문 분야에서 역량을 발휘하도록 돕고 있습니다.

### PECB 의 주요 목표는 다음과 같습니다:

1. 전문가를 인증하고 자격을 부여하는 데 필요한 최소한의 요구사항을 수립
2. 개인의 자질을 검토하고 검증하여 인증 자격에 적합한지 확인
3. 개인 인증을 위한 평가 프로세스의 유지 및 지속적인 개선
4. 자격을 갖춘 개인을 인증하고, 자격을 부여하고, 각 디렉토리를 유지관리
5. 인증의 정기적인 갱신 요건을 수립하고 인증된 개인이 이러한 요구사항을 준수하는지 확인
6. PECB 전문가가 업무 수행 시 윤리 기준을 충족하는지 확인
7. 공동의 이해관계가 있는 사안에 대해 이해당사자 대변
8. 전문가, 기업, 정부 및 대중에게 인증 및 자격증 프로그램의 혜택 홍보

### 미션

신뢰를 강화하는 종합적인 시험, 자격인증, 자격증 프로그램을 고객에게 제공함으로써 사회 전체에 기여한다.

### 비전

전문 자격인증 서비스 및 자격증 프로그램 제공의 글로벌 기준이 된다

### 가치

청렴, 프로페셔널리즘, 공정

## PECB 인증의 가치

### 글로벌 인지도

PECB 자격증은 많은 인증 기관에서 국제적으로 인정하고 보장하므로, 자격증을 취득한 전문가는 국내 및 국제 시장에서 인정받는 혜택을 누릴 수 있습니다.

PECB 인증의 가치는 ISO/IEC 17024 - 개인에 대한 인증을 운영하는 기관에 대한 일반 요구사항에 따라 국제인증기구(IAS-PCB-111), 영국인증기구(UKAS-No. 21923) 및 한국인증기구(KAB-PC-08)의 인증을 통해 검증됩니다. PECB 인증 프로그램의 가치는 ANSI/ASTM E2659-18, 인증 프로그램에 대한 표준 관행에 따라 ANSI 국가인증위원회(ANAB-Accreditation ID 1003)의 인증을 통해 검증됩니다.

PECB 는 국제공인등특기관협회(IAAR)의 준회원, 국제인적자원인증협회(IPC)의 정회원, IPC MLA 의 서명 회원, 클럽 EBIOS, CPD 인증 서비스, CLUSIF, Credential Engine 및 ITCC 의 회원입니다. 또한 PECB 는 사이버보안 성숙도 모델 인증 표준(CMMC)에 대해 사이버보안 성숙도 모델 인증 기관(CMMC-AB)으로부터 공인 파트너 인증기관(LPP)으로 승인받았으며, 클럽 EBIOS 로부터 EBIOS 리스크 관리자 기술 인증을 제공하고, CNIL(프랑스 정보자유위원회)로부터 DPO 인증을 제공하도록 승인받았습니다. 자세한 내용은여기를 클릭하십시오.

### 고품질 제품 및 서비스

당사는 고객의 요구와 필요에 맞는 고품질의 상품과 서비스를 제공하는 것을 자랑스럽게 생각합니다. 당사의 모든 제품은 우수관행과 방법론을 바탕으로 전문가와 실무진으로 구성된 팀이 신중하게 준비합니다.

### 표준 준수

당사의 자격인증 및 자격증 프로그램은 ISO/IEC 17024 및 ASTM E2659 를 준수하고 있음을 입증합니다. 인증은 표준의 요건이 충분한 일관성, 프로페셔널리즘, 공정성을 바탕으로 충족 및 검증되었다는 의미입니다.

### 고객 중심 서비스

PECB 는 고객중심 기업으로, 모든 고객을 가치 있고 소중하게, 또한 프로페셔널하고 정직하게 대합니다. PECB 는 요청사항,질문 및 요구사항을 전담하는 전문팀을 보유하고 있습니다. PECB 는 서비스의 품질을 유지하는 선에서 최대 24 시간 이내에 대응하고자 최선을 다하고 있습니다.

### 유연성과 편리함

온라인 학습 기회는 귀하의 라이프스타일에 따라 학습 과정 일정을 잡을 수 있기에 귀하의 전문가로서의 여정을 더욱 편리하게 이어 줍니다. 이러한 유연성은 귀하께 더 많은 자유 시간을 제공하고, 더 많은 경력 발전 기회를 제공하며, 비용을 절감하도록 해줍니다.

## PECB 윤리강령(Code of Ethics)

윤리강령은 서비스를 제공하고 고객을 유지할 때 윤리강령의 중요성을 인식하여 PECB 가 준수하기 위해 전적으로 헌신하는 최고의 가치와 윤리를 나타냅니다.

컴플라이언스 부서는 PECB 직원, 강사, 시험출제자, 시험감독관, 파트너, 유통업체, 각종 자문위원회 및 위원회 위원, 인증된 개인 및 자격증 보유자(이하 "PECB 프로페셔널")가 본 윤리강령을 준수하도록 합니다. 또한 컴플라이언스 부서는 신청자, 수강생, 인증된 개인, 인증서 보유자, 인정기관, 정부기관과 같은 내외부 이해관계자에게 서비스를 제공할 때 전문성을 갖추고 전적인 책임과 역량, 공정성을 갖고 행동해야 함을 일관되게 강조합니다.

PECB 는 조직의 성공을 달성하려면 클라이언트와 이해관계자의 요구 사항과 기대치를 완전히 이해해야 한다고 믿습니다. 이를 위해 PECB 는 최고 수준의 무결성, 전문성, 공정성을 기반으로 문화를 조성하며, 이는 PECB 의 가치이기도 합니다. 이러한 가치는 조직에 필수적이며 수년에 걸쳐 전 세계적인 입지와 성장을 특징지었고 PECB 가 오늘날 누리고 있는 명성을 확립했습니다.

PECB 는 튼튼한 윤리적 가치가 건강하고 강한 관계를 맺는 데 필수적이라고 믿습니다. 따라서 PECB 의 주요 책임은 PECB 전문가가 PECB 원칙과 가치를 완전히 준수하는 행동을 보이도록 하는 것입니다.

PECB 전문가는 다음을 준수합니다:

1. 서비스 제공에 있어 정직, 정확성, 공정성 및 독립성에 기반한 전문적인 행동을 합니다
2. 본 윤리강령 및 기타 전문 표준에 따라 항상 고용주, 고객, 대중 및 자신의 직업에 가장 큰 이익을 제공하기 위해 노력합니다
3. 각자의 분야에서 역량을 발휘하고 개발하며 지속적으로 기술과 지식을 향상시키기 위해 노력합니다
4. 자격과 역량을 갖춘 사람에게만 서비스를 제공하고, 관련 우려 사항이나 리스크를 포함하여 서비스의 성격에 대해 클라이언트와 고객에게 올바르게 알립니다
5. 고용주나 클라이언트에게 판단에 영향을 미치거나 이를 훼손할 수 있는 비즈니스 이해관계나 제휴를 알립니다
6. 서비스 제공 중 현재 또는 이전 고용주나 클라이언트 정보의 기밀성을 유지합니다
7. 서비스 제공이 수행된 국가 관할권의 모든 관련 법률 및 규정은 준수합니다
8. 타인의 지적재산과 기여를 존중합니다

9. PECB 자격인증 또는 PECB 자격증 프로그램 신청자에 대한 평가 프로세스의 무결성을 손상시킬 수 있는 허위 또는 왜곡된 정보를 고의적으로 전달하지 않기
10. 정식 라이선스 없이 자신을 PECB 대표로 허위 또는 잘못 표시하거나 PECB 로고, 인증 또는 인증서를 오용하지 않기
11. PECB의 명성, 자격인증 또는 자격증 프로그램을 손상시킬 수 있는 방식으로 행동하지 않기
12. 본 윤리강령의 침해 주장에 따른 조사에 전적으로 협조하기

PECB 윤리강령 전문을 읽으려면 [Code of Ethics | PECB](#)로 이동하십시오.



## ISO/IEC 27001 선임심사원 소개

ISO/IEC 27001 은 정보보호 경영시스템(ISMS)의 수립, 실행, 유지, 지속적 개선에 필요한 요구사항을 규정합니다. 조직은 ISMS 를 실행하는 것 외에도 실행한 통제 또는 프로세스가 의도한 결과를 가져오는지에 대한 확신이 필요합니다. 심사를 통해 조직은 시행중인 ISMS 의 효과를 평가하고 이를 더욱 개선할 수 있습니다.

PECB 에서 제공하는 교육 과정을 통해 수강생은 ISO/IEC 27001 의 인증 프로세스에 따라 심사를 효과적으로 계획 및 수행하고, 심사 기법과 관행을 적용하며, 심사팀 및 심사 프로그램 관리(또는 참여)할 수 있는 역량을 강화 할 수 있습니다.

심사가 가장 수요가 많은 직업 중 하나라는 점을 고려할 때, 국제적으로 인정받는 자격증을 취득하면 직업적 목표를 달성하는데 도움이 될 수 있습니다. 'ISO/IEC 27001 선임심사원' 인증은 정보보호 경영시스템을 심사하고 심사팀을 주도할 수 있는 역량을 증명하고자 하는 개인을 위한 전문 자격증입니다.

PECB 자격인증은 라이선스나 단순 멤버십이 아닙니다. 수강생이 교육과정을 통해 습득한 지식과 기술을 증명하며, 필요한 경력을 갖추고 시험에 합격한 응시자에게 발급됩니다.

본 문서는 ISO/IEC 17024:2012 를 준수하는 PECB ISO/IEC 27001 선임심사원(Lead Auditor) 인증제도를 명시하고 있습니다. 본 수강생 핸드북에는 수강생이 증명서를 획득하고 유지할 수 있는 단계에 대한 정보도 포함되어 있습니다. 지원서를 작성 및 제출하기 전에 반드시 본 수강생 핸드북의 모든 내용을 읽어보시기 바랍니다. 수강생 핸드북을 읽고나서 문의사항이 있으시면 PECB 국제사무소 [certification.team@pecb.com](mailto:certification.team@pecb.com) 로 연락주시기 바랍니다.

## 제 2 장: 시험 준비, 규칙 및 정책

---

### 시험준비 및 일정 등록

모든 응시자는 자신의 학습 및 자격인증 시험 준비에 있어 스스로 책임을 져야 합니다. 응시자가 반드시 교육 과정에 참석해야만 시험에 응시할 수 있는 것은 아니지만, 교육 과정에 참석하면 시험에 합격할 확률이 크게 높아집니다.

시험 일정을 잡으려면 응시자에게는 두 가지 옵션이 있습니다:

1. 공인 파트너 중 한 곳에 문의합니다. 해당 지역의 공인 파트너를 찾으려면 [액티브 파트너](#)로 이동하세요. 교육 과정 일정은 온라인으로도 확인할 수 있으며 [강좌 이벤트](#) 강좌 이벤트에서 확인할 수 있습니다. 서 확인할 수 있습니다.
2. [PECB 시험 애플리케이션](#)을 통해 원격으로 PECB 시험에 응시하세요. 원격 시험 일정을 예약하려면 다음 링크로 이동하세요: [시험](#).

시험, 역량분야, 지식에 관한 더욱 상세한 정보는 본 문서의 제 3 장을 참조하시기 바랍니다.

### 시험 일정 변경

시험 일자, 시간, 장소 혹은 기타 자세한 사항에 관한 문의는 다음으로 문의바랍니다. [online.exams@pecb.com](mailto:online.exams@pecb.com)

### 시험 및 인증 신청 비용

강좌를 수강하지 않아도 PECB 시험에 응시할 수 있습니다. 비용은 다음과 같습니다:선임(Lead) 인증시험: \$1000<sup>1</sup>

- 관리자(Manager) 인증시험: \$700
- 기본(Foundation)시험: \$500
- 전환(Transition) 시험: \$500

인증 신청비는 미화 500 달러입니다.

PECB 파트너 중 한 곳을 통해 교육 과정에 참여한 응시자의 경우, 신청 수수료에는 시험 비용(첫 번째 시험 및 첫 번째 재응시), 인증 신청서, 첫 해 연간갱신비(Annual Maintenance Fee, AMF)가 포함됩니다.

---

<sup>1</sup>이 문서에 기재된 모든 가격은 미국 달러 기준입니다.

## 역량 영역

‘ISO/IEC 27001 선임심사원’ 인증은 정보보호 경영시스템을 심사하고 심사팀을 주도할 수 있는 역량을 증명하고자 하는 개인을 위한 전문 자격증입니다.

시장에서 요구되는 가장 중요한 기술은 인증 프로세스에 따라 효과적으로 심사를 계획 및 수행하고, 심사 기법과 관행을 적용하며, 심사팀과 심사 프로그램을 관리(또는 참여)하는 능력입니다.

ISO/IEC 27001 선임심사원 인증은 다음과 같은 개인에게 적합합니다: 정보보호 경영시스템(ISMS) 심사를 수행하고 주도하고자 하는 심사원

- 정보보호 경영시스템 심사 프로세스를 마스터하고자 하는 관리자 혹은 컨설턴트
- 조직 내에서 ISMS 요구사항 준수 유지를 담당하는 개인
- 정보보호 경영시스템 심사를 준비하고자 하는 기술 전문가
- 정보보호 경영 전문위원

시험 내용은 다음과 같이 구분됩니다:

- **영역 1:** ISMS 의 기본 원칙과 개념
- **영역 2:** 정보보호 경영시스템(ISMS)
- **영역 3:** 심사의 기본 개념과 원칙
- **영역 4:** ISO/IEC 27001 심사 준비
- **영역 5:** ISO/IEC 27001 심사 실행
- **영역 6:** ISO/IEC 27001 심사 종료
- **영역 7:** ISO/IEC 27001 심사 프로그램 관리

## 영역 1: ISMS 의 기본 원칙과 개념

주요 목표: ISO/IEC 27001 원칙 및 개념을 설명하고 적용할 수 있는지 확인 할 수 있다.

역량	지식
1. 정보보호 경영시스템의 주요 개념을 이해 및 설명하는 능력	1. 조직이 준수해야 하는 정보보호 법, 규정, 국제 및 산업 기준, 계약, 시장 관행, 내부 정책 등에 관한 지식
2. 조직의 운영 및 정보보호 표준 개발을 이해 및 설명하는 능력	2. 정보보호과 관련된 주요 표준에 관한 지식
3. 조직을 위한 정보보호 컴플라이언스 요구사항을 식별, 분석, 평가하는 능력	3. ISO/IEC 27001 의 주요 개념 및 용어에 관한 지식
4. 정보보호 및 정보보호 리스크 관리의 주요 개념을 설명 및 명확히 하는 능력	4. 정보보호의 리스크 개념 및 그 적용에 관한 지식
5. 정보 자산, 데이터, 기록의 차이점을 구별 및 설명하는 능력	5. 정보보호 측면 간 관계에 관한 지식
6. 통제, 취약점, 위협, 리스크, 자산과 같은 정보보호 측면 간 관계를 이해, 해석 및 명확히 하는 능력	6. 보안 목표 및 통제의 차이점 및 특징에 관한 지식
7. 빅데이터, 인공지능, 머신러닝, 클라우드 컴퓨팅, 업무 아웃소싱을 식별 및 명확히 하는 능력	7. 예방, 탐지, 시정 통제의 차이점에 관한 지식
	8. 빅데이터, 인공지능, 머신러닝, 클라우드 컴퓨팅, 업무 아웃소싱의 주요 특징에 관한 지식

## 영역 2: ISMS 및 ISO/IEC 27001 입문 요구사항

주요 목표: ISO/IEC 27001 을 바탕으로 정보보호 경영시스템을 위한 요구사항을 파악하고 설명할 수 있다.

역량	지식
1. ISO/IEC 27001:2022 표준의 구조를 이해하는 능력	1. ISO/IEC 27001:2022 표준 및 지원 표준에 대한 지식
2. ISO/IEC 27001 및 그 주요 프로세스를 바탕으로 정보보호 경영시스템의 구성 요소를 이해하는 능력	2. 경영시스템과 관련된 개념, 원칙, 용어에 관한 지식
3. ISO/IEC 27001 요구사항을 이해, 해석, 분석하는 능력	3. 통합 경영시스템의 주요 특징에 관한 지식
4. 조직의 ISMS 를 수립, 실행, 운영, 모니터링, 검토, 유지 및 개선하기 위한 주요 단계를 이해, 설명 및 명확히 하는 능력	4. 4 절~10 절에 제시된 ISO/IEC 27001 요구사항에 관한 지식
5. ISMS 와 관련된 외부 및 내부 요인을 파악하고 이해관계자 및 요구 사항을 결정하는 능력	5. ISO/IEC 27001 부속서 A 에 나열된 93 개 통제에 관한 지식
6. ISMS 의 범위를 결정하는 능력	6. ISMS 내부 및 외부 요인 및 이해관계자에 대한 지식
7. 관리자의 의지를 확인하고, 정보보호 정책을 수립하며, ISMS 의 역할과 책임을 할당하는 능력	7. ISMS 범위 및 정보보호 정책을 수립하기 위한 주요 단계에 대한 지식
8. 변경 사항 및 리스크에 대처하기 위한 조치를 계획할 수 있는 능력	8. 최고 경영진의 리더십과 의지, ISMS 와 관련된 조직의 역할과 책임에 대한 지식
9. 리스크 평가 및 리스크 처리 프로세스를 이해하는 능력	9. 조직의 전반적 정책 및 목표에 따라 결과를 제공하기 위해 리스크를 관리하고 및 정보보호를 개선하는 것과 관련된 보안 목표, 프로세스 및 절차에 대한 지식
10. ISO/IEC 27001 부속서 A 및 기타 출처를 바탕으로 적절한 통제의 선택을 이해하는 능력	10. 리스크 평가 및 처리 접근 방식과 방법론에 관한 지식
11. 직원이 ISMS 관련 업무를 수행할 수 있는 인식과 역량을 갖추었는지 확인할 수 있는 능력	11. 부속서 A 통제 및 기타 출처에 반한 추가 통제의 선택과 적용성 보고서에 포함되는 것에 대한 지식
12. ISMS 의 성과를 모니터링 및 평가하고 내부 심사 및 관리 검토를 수행할 수 있는 능력	

- 
- |  |   |
|--|---|
| <p>13. 지속적인 개선을 보장하고 부적합 사항을 처리하기 위한 올바른 조치를 이행할 수 있는 능력</p> | <p>12. 모니터링, 측정, 분석 및 평가, 내부 심사 및 경영진 검토를 포함한 성과 평가 프로세스에 대한 지식</p> <p>13. 지속적 개선의 개념 및 ISMS 에 대한 적용에 관한 지식</p> |
|--|---|

## 영역 3: 심사의 기본 개념과 원칙

주요 목표: ISMS 심사와 관련된 주요 개념 및 원칙을 해석하고 적용할 수 있다.

역량	지식
1. ISMS 심사에서 심사 원칙의 적용을 이해, 설명 및 명확히 하는 능력	1. ISO 19011 에 명시된 주요 심사 개념 및 용어에 관한 지식
2. '자체 심사, 제 2 자 심사, 제 3 자 심사를 구별하는 능력'	2. 자체 심사, 제 2 자 심사, 제 3 자 심사의 차이점에 관한 지식
3. 심사원의 전문성에 대한 평판을 실추하고 PECB 윤리강령(Code of Ethics)을 위반하는 상황을 식별 및 판단하는 능력	3. 심사의 원칙(무결성, 공정공시, 전문가로서 갖추어야 할 소양, 기밀성, 독립성, 증거기반 접근법, 리스크 기반 접근법)에 관한 지식
4. 심사 고객, 피심사조직, 법률 집행, 규제 당국과 관련된 의무를 고려하는 윤리적 이슈를 식별 및 판단하는 능력	4. 심사원의 직업적 책임 및 PECB 윤리강령(Code of Ethics)에 관한 지식
5. 피심사조직이 저지른 부정행위와 관련된 법적 영향에 대해 심사원이 취해야 할 조치를 이해하는 능력	5. 심사의 증거기반 접근법에 관한 지식
6. ISMS 심사의 맥락에서 증거기반 접근법을 설명, 적용 및 명확히 하는 능력	6. 다른 유형의 심사 증거(물리적, 수학적, 확증적, 기술적, 분석적, 문서적, 구술적 심사 근거)에 관한 지식
7. 증거 유형 및 그 특징을 설명 및 비교하는 능력	7. 피심사조직 및 해당 법률 및 규제를 적용하는 국가 등에 적용 가능한 법률 및 규제에 관한 지식
8. ISMS 심사에서 요구하는 증거의 종류 및 양을 결정 및 판단하는 능력	8. 심사의 빅데이터 사용에 관한 지식
9. 심사 트렌드와 기술의 영향을 이해하는 능력	9. 업무 아웃소싱의 심사에 관한 지식

## 영역 4: ISO/IEC 27001 심사 준비

주요 목표: 정보보호 경영시스템 심사를 준비할 수 있다.

역량	지식
1. 심사의 구체적 맥락을 고려하는 ISMS 심사를 준비하기 위한 단계 및 활동을 이해 및 명확히 하는 능력	1. 심사 계획 준비 절차에 관한 지식
2. ISMS 심사의 다른 단계 중 중요성 수준을 결정 및 평가하고 리스크 기반 접근법을 적용하는 능력	2. 심사에 대한 리스크 기반 접근법 및 내재된 리스크, 통제 리스크, 탐지 리스크와 같은 심사 활동과 관련된 다른 유형의 리스크에 관한 지식
3. ISMS 심사에서 요구되는 적절한 수준의 합당한 보증을 판단하는 능력	3. 중요성의 개념 및 심사에 대한 적용에 관한 지식
4. 심사팀장, 심사팀 구성원, 기술 전문가의 역할과 책임을 이해 및 설명하는 능력	4. 합당한 보증의 개념 및 심사에 대한 그 적용에 관한 지식
5. 심사 타당성을 결정하는 능력	5. 심사팀장, 심사팀 구성원, 기술 전문가의 역할과 책임을 이해 및 설명하는 능력
6. ISMS 심사를 위한 심사 목적, 심사 기준, 심사 범위를 결정, 평가 및 확인하는 능력	6. 심사 목적, 심사 범위, 심사 기준에 관한 지식
7. 심사 참여의 용어의 특징을 설명, 정의 및 명확히 하고 피심사조직과 최초로 접촉하기 위한 우수 관행을 적용하는 능력	7. ISMS 범위와 심사 범위의 차이점에 관한 지식
	8. 심사 타당성 동안 고려할 요인에 관한 지식
	9. 심사에서 고려할 문화적 측면에 관한 지식
	10. 심사 참여의 용어의 특징 및 피심사조직과 최초로 접촉하기 위한 우수 관행에 관한 지식



## 영역 5: ISO/IEC 27001 심사 실행

주요 목표: ISMS 심사를 수행할 수 있다.

역량	지식
1. 문서화된 정보 평가 기준을 고려하여 1 단계 심사를 수행하는 능력	1. 심사 시작회의의 목적 및 내용에 관한 지식
2. 시작회의를 조직 및 수행하는 능력	2. 1 단계 심사와 2 단계 심사의 차이점에 관한 지식
3. 해당 단계가 수반하는 절차를 적절하게 준수하여 2 단계 심사를 수행하는 능력	3. 1 단계 심사의 요구사항, 단계, 활동에 관한 지식
4. 적절한 심사 증거를 수집하기 위한 의사소통 우수 관행을 적용하는 능력	4. 문서화된 정보 평가 기준 및 ISO/IEC 27001 요구사항에 관한 지식
5. 모든 관련 이해당사자들의 역할 및 책임을 고려하는 능력	5. 2 단계 심사의 요구사항, 단계, 활동에 관한 지식
6. 증거 수집 절차 및 도구를 설명, 적용 및 명확히 하는 능력	6. 심사 중 우수 의사소통 관행에 관한 지식
7. 주요 심사 샘플링 방법을 설명, 적용 및 명확히 하는 능력	7. 심사 중 안내자 및 참관인의 역할 및 책임에 관한 지식
8. 심사 중 이용 가능한 정보에서 적절한 증거를 수집하고 이를 객관적으로 평가하는 능력	8. 다른 분쟁 해결 테크닉에 관한 지식
9. ISMS 심사에서 심사 작업문서를 개발하고 적절한 심사 시험 계획을 상술하는 능력	9. 인터뷰, 문서화된 정보 검토, 관찰, 분석, 샘플링, 기술적 검증과 같은 근거 수집 절차 및 도구에 관한 지식
10. 심사 결과 작성에 대한 증거 평가 프로세스를 설명하고 적용할 수 있는 능력	10. 증거 분석 테크닉(확증 및 평가)에 관한 지식
11. 무죄추정의 원칙에 대한 개념을 이해, 설명 및 명확히 하는 능력	11. 심사에서 사용한 주요 개념, 원칙, 증거 수집 절차에 관한 지식
12. 심사 규칙 및 원칙에 따라 적절한 심사 관찰을 보고하는 능력	12. 심사 체크리스트 사용의 장점 및 단점에 관한 지식
13. 심사 문서에 대한 심도 있는 검토를 수행하는 능력	13. 주요 심사 샘플링 방법 및 그 특징에 관한 지식
14. 심사 업무 문서를 작성하는 능력	14. 심사 계획 준비 절차에 관한 지식
	15. 심사 작업문서의 준비 및 개발에 관한 지식
	16. 심사 시험 계획의 생성을 위한 우수 관행에 관한 지식
	17. 증거 평가 프로세스(심사 결과 수립)에 관한 지식

## 영역 6: ISO/IEC 27001 심사 종료

주요 목표: ISMS 심사를 완료하고 심사 후속 활동을 수행할 수 있다.

역량	지식
1. 증거 평가 프로세스(심사 결론 준비)를 설명 및 적용하는 능력	1. 심사 결론을 작성하기 위한 증거 평가 프로세스에 대한 지식
2. 인증 권고를 판단하는 능력	2. 심사 결론 제시에 관한 지식
3. 심사 결론을 작성 및 제시하는 능력	3. 피심사조직 조직의 관리에 대한 심사 결론을 제시하기 위한 가이드라인 및 우수관행에 관한 지식
4. 종결회의를 조직 및 수행하는 능력	4. 인증심사 중 심사원이 발표할 수 있는 권고사항에 관한 지식
5. ISO/IEC 27001 심사보고서를 작성 및 배포하는 능력	5. 종결회의 의제에 관한 지식
6. 조치계획을 평가하는 능력	6. 조치계획을 평가하기 위한 가이드라인 및 우수관행에 관한 지식

## 영역 7: ISO/IEC 27001 심사 프로그램 관리

주요 목표: ISMS 심사 프로그램을 수립하고 관리할 수 있다.

역량	지식
1. 심사 후속조치 및 점검활동을 포함한 최초 심사에 뒤따르는 활동을 수행하는 능력	1. 심사 후속조치, 사후심사, 갱신심사 요구사항, 단계, 활동에 관한 지식
2. 심사 프로그램의 수립 및 심사 프로그램에 대한 PDCA 사이클의 적용을 이해 및 설명하는 능력	2. 조직의 인증의 변경, 확장, 효력정지 혹은 철수를 위한 조건에 관한 지식
3. 심사 기록의 무결성, 가용성, 기밀성 보호의 중요성 및 이 점에서의 심사원의 책임을 이해 및 설명하는 능력	3. 심사 프로그램 관리의 PDCA 사이클의 적용에 관한 지식
4. 심사 기록의 무결성, 가용성, 기밀성 보호의 중요성을 이해 및 설명하는 능력	4. 심사 자원, 절차, 정책과 관련된 요구사항, 가이드라인, 우수관행에 관한 지식
5. 5. 품질 관리, 기록 관리, 민원 관리와 같은 심사 프로그램 경영시스템의 구성 요소와 관련된 요구사항을 이해하는 능력	5. 전문 심사원이 사용하는 도구의 종류에 관한 지식
6. 6. 심사 프로그램에서 통합심사가 이루어지는 방법을 이해 및 설명하는 능력	6. 심사 기록 관리와 관련된 요구사항, 가이드라인, 우수관행에 관한 지식
7. 문서화된 정보 관리 프로세스를 이해하는 능력	7. 심사 프로그램 관리에 대한 지속적 개선의 적용에 관한 지식
8. 각각의 심사원 및 심사팀 구성원의 성과를 모니터링함으로써 심사 프로그램의 효율성을 평가하는 프로세스를 이해하는 능력	8. 자체 심사, 제 2 자 심사, 제 3 자 심사 프로그램을 실행 및 관리하기 위한 세부 사항에 관한 지식
9. 전문 심사원과 관련된 개인적 특성 및 행동의 적용을 증명하는 능력	9. 통합심사의 관리에 관한 지식
	10. 전문 심사원의 개인적 특성 및 행동에 관한 지식

위에 언급한 영역과 그 적합성에 따라 시험은 아래 표에 요약된 대로 객관식 80 문항으로 구성됩니다:

	역량 영역별 문항 수와 배점	역량 영역별 배점 비중(%)	요구되는 이해 수준(인지/분류)		
			이해, 적용, 분석을 측정하는 문항	평가를 측정하는 문항	
ISO/IEC 27001 영역	ISMS 의 기본 원칙과 개념	13 장	16.25 장	X	
	ISMS 및 ISO/IEC 27001 입문 요구사항	8 장	10 장	X	
	심사의 기본 개념과 원칙	14 장	17.5 장		X
	ISO/IEC 27001 심사 준비	12 장	15 장	X	
	ISO/IEC 27001 심사 실행	18 장	22.5 장		X
	ISO/IEC 27001 심사 종료	7 장	8.75 장	X	
	ISO/IEC 27001 심사 프로그램 관리	8 장	10 장		X
	합계	<b>80 장</b>	<b>100%</b>		
이해 수준별 문항의 수			<b>40 장</b>	<b>40 장</b>	
각 이해 수준의 비중(인지/분류)			<b>50%</b>	<b>50%</b>	

합격기준은 70% 입니다.

시험 합격 후, 응시자는 'PECB 인증 ISO/IEC 27001 선임심사원' 자격증명 취득을 위한 신청을 할 수 있습니다.

## 시험 응시

### 시험에 관한 일반 정보

응시자는 시험 시작 30 분 전까지 시험장에 입장해야 합니다.

지각자에게 지연된 시간에 대한 보상은 주어지지 않으며, 시험 응시가 거부될 수 있습니다.

응시자는 유효한 신분증(국가 신분증, 운전면허증, 여권)을 지참하고 감독관에게 제시해야 합니다.

모국어가 아닌 언어로 시험(지필시험)에 응시하는 경우, 시험 당일 요청이 있으면 다음과 같이 추가 시간이 제공될 수 있습니다.

- 기본 시험: 10 분 추가
- 관리자 시험: 20 분 추가
- 선임 시험: 30 분 추가

### PECB 시험 형식 및 유형

1. **지필시험:** 시험지는 종이 형태로 제공되며, 응시자는 배부된 시험지와 필기구만 사용할 수 있습니다. 노트북, 태블릿 PC, 휴대전화 등의 전자기기는 사용할 수 없습니다. 시험 세션은 파트너가 강좌를 주최한 장소에서 PECB 승인 감독관이 감독합니다.
2. **온라인 시험:** 시험은 PECB 시험 어플리케이션을 통해 제공됩니다. 휴대전화나 태블릿 PC 등의 전자기기는 사용할 수 없습니다. 시험 세션은 PECB 시험 어플리케이션과 외장/내장 카메라를 통해 PECB 감독관이 원격으로 감독합니다

온라인 시험에 대한 자세한 내용은 [PECB 온라인 시험 가이드](#)를 참조하세요.

PECB 시험은 두 가지 유형으로 제공됩니다:

1. 주관식 문제 시험
2. 객관식 문제 시험

**본 시험은 객관식 문제로 구성됩니다.** 객관식 시험을 통해 간단하고 복잡한 개념을 포함한 다양한 주제에 대한 응시자의 이해도를 평가할 수 있습니다. 이 시험은 단독 문항 및 시나리오 기반 문제로 구성됩니다. 단독 문항은 시험 내에서 독립적으로 출제되며 문맥에 의존하지 않는 반면, 시나리오 기반 문제는 문맥에 의존하며, 즉 응시자가 읽어야 하는 시나리오 기반으로 개발되어 해당 시나리오와 관련된 5 개의 질문에 대한 답을

제공해야 합니다. 단독 문항 및 시나리오 기반 문제에 답할 때 응시자는 교육 과정에서 설명된 다양한 개념과 원리를 적용하고, 문제를 분석하고, 대안을 식별 및 평가하고, 여러 개념이나 아이디어를 결합하는 등의 작업을 수행해야 합니다.

각 객관식 문제에는 세 가지 옵션이 있으며, 이 중 하나는 정답이고 두 개는 오답입니다.

본 시험은 오픈북 시험입니다. 응시자가 참조할 수 있는 자료는 다음으로 한정됩니다:

- 하드카피로 출력된 ISO/IEC 27001 표준
- 강좌 교재(PECB 시험 앱 또는 출력본)
- 강좌 수강 중 작성된 개인 메모 (PECB 시험 앱 또는 출력본)
- 종이 사전

시험 문제 샘플은 아래에 제공됩니다.

**비고:** PECB 는 점차적으로 객관식 시험으로 전환될 예정입니다. 또한 오픈북 형태로 PECB 가 응시자의 지식, 능력, 새로운 상황에서 정보를 이용할 수 있고(적용), 아이디어 간의 연결고리를 찾을 수 있으며(분석), 입장 혹은 결정의 근거를 설명할 수 있는(평가) 스킬을 평가할 것입니다.

시험 유형, 지원 언어 및 기타 세부 사항에 대한 구체적인 정보는 [examination.team@pecb.com](mailto:examination.team@pecb.com) 으로 문의하거나 [PECB 시험 목록](#)으로 이동하세요.

## 시험 문제 샘플

회사 A 는 시카고에 본사가 있는 보험사다. 회사는 의료 및 자동차 보험을 포함한 다양한 종류의 서비스와 상품을 제공한다. 최근에 회사는 가장 성공적이고 규모도 큰 보험사가 되어 전국적으로 70 개가 넘는 지사를 보유하게 되었다.

회사의 목표는 자산을 제대로 유지하고 고객 정보의 기밀성을 보호하는 것이다. 회사가 ISO/IEC 27001 에 대한 인증을 받기로 결정한 이유는 이를 통해 목표를 달성하고 국제법과 규제를 준수할 뿐만 아니라 평판을 높일 수 있기 때문이다. 회사는 기존 프로세스 및 ISMS 요구사항에 대한 상세한 분석을 기반으로 실행 전략을 정의함으로써 ISMS 실행을 시작하였다. 회사는 직면하고 있는 위협 및 취약점을 이해하는 데 핵심적인 정보보호 리스크 평가에 특히 집중하였다. 회사는 식별된 리스크를 평가할 목적으로 리스크 기준 또한 정의하였다.

회사 A 의 급속 성장은 복잡하고 집약적인 데이터 프로세싱이라는 결과를 초래했으며, 리스크 평가 결과를 바탕으로 우선 기존 정보분류체계를 업데이트하고 정보의 각 분류에 요구되는 보호 수준을 기반으로 필요한 보안 통제를 실행하기로 했다.

민감 정보로 분류되는 고객의 의료비 청구 내역은 AES 암호화를 사용해 암호화되고 프라이빗 클라우드로 이동되었다. 회사 A 는 편리한 액세스를 위해 클라우드 저장소를 사용하였다. 직원들이 서비스에 자주 액세스하기 때문에 회사는 로그인 프로세스 또한 사용하기로 하였다. 의료비 청구 내역을 담당하는 모든 직원이 자동으로 클라우드 저장소에 액세스할 수 있도록 서비스를 설정하였다.

클라우드 저장 서비스가 사람의 오류 혹은 의도적 공격으로 보안 침해를 겪었기 때문에, 회사의 IT 부서는 업무 이메일이 사용되지 않은 경우 클라우드에 저장된 민감 정보에 대한 액세스를 제한하기로 결정했다. 또한 암호 관리 소프트웨어를 사용하여 이러한 이메일 주소의 암호를 관리하고 더 강도 높은 암호를 생성하도록 했다.

위 시나리오를 바탕으로 다음에 답하십시오.

1. IT 부서는 클라우드 저장소에 대한 액세스를 제한하지 않았다. 다음 중 어떤 위협이 이러한 취약점을 악용할 수 있는가?
  - A. 하드웨어 변조(tampering)
  - B. **민감 정보의 미승인 사용**
  - C. 불충분한 클라우드 저장소 교육

2. 회사 A 는 클라우드로 옮기기 전에 민감 정보를 암호화한다. 이 경우 어떤 정보보호 원칙이 준수되고 있는가?
  - A. 기밀성—암호화를 실행하면 권한이 있는 사용자만 암호화된 정보에 액세스할 수 있다.
  - B. 가용성—암호화는 정보가 비활성화 상태이든 전송 상태이든 상관없이 보호되도록 보장하며 따라서 필요할 경우 액세스할 수 있다.
  - C. 무결성—암호화는 암호화된 정보에 승인된 수정만 이루어지도록 한다.
  
3. 회사 A 는 업무 이메일이 사용되지 않았을 경우 클라우드에 저장된 민감 정보에 대한 액세스를 제한하기로 결정하였다. 이 경우 어떤 보안 통제가 실행되었는가?
  - A. 탐지 통제
  - B. 예방 통제
  - C. 시정 통제
  
4. 회사 A 는 리스크 평가 시 리스크 기준을 정의하였다. 이는 필요한 조치인가?
  - A. 예—회사는 정보보호 리스크를 평가할 때 리스크 기준을 수립 및 유지해야 한다.
  - B. 아니오—리스크 기준은 리스크 처리 옵션이 정의되었을 때만 수립되어야 한다.
  - C. 아니오—리스크 기준은 정보보호 잔여 리스크가 수용되었을 때 수립된다.



## 시험 보안 정책

PECB 는 시험과 시험 과정 전반의 무결성을 보호하기 위해 최선을 다하고 있으며, 지원자, 잠재적 지원자, 응시자 및 파트너의 윤리적 행동에 의존하여 PECB 시험의 기밀을 유지합니다. 이 정책은 허용되지 않는 행동에 대처하고 모든 응시자를 공정하게 대우하는 것을 목표로 합니다.

PECB 시험 내용에 대한 정보를 공개하는 행위는 본 정책과 PECB 윤리 강령을 전면으로 위반하는 것입니다. 따라서 PECB 시험에 응시하는 응시자는 시험 기밀 유지 및 비공개 동의성에 서명해야 하며, 다음 사항을 준수해야 합니다:

1. 시험 자료의 문제와 답은 PECB 의 독점, 기밀 자산입니다. 응시자가 PECB 에 시험 제출을 완료하면 더 이상 시험 원본이나 사본에 액세스 할 수 없습니다.
2. 응시자는 시험의 문제와 정답에 관한 정보를 공개하거나 다른 응시자 또는 다른 사람과 관련 세부 사항을 논의 할 수 없습니다.
3. 응시자는 시험과 관련된 모든 자료를 시험장 밖으로 가져갈 수 없습니다.
4. 응시자는 문제, 답안 또는 화면 이미지를 포함하여 시험 자료를 복사하거나 복사하려고 시도할 수 없습니다. (작성, 복사 또는 기타 방식에 관계없이)
5. 응시자는 다음과 같은 시험 부정행위에 참여하거나 이를 조장해서는 안 됩니다:
  - 다른 응시자의 시험 자료 또는 답안지를 보는 행위
  - 감독관, 응시자 또는 다른 사람으로부터 도움을 주거나 받는 행위
  - PECB 가 승인하지 않은 "브레인 덤프" 사이트 사용을 포함하여 승인되지 않은 참고 가이드, 매뉴얼, 도구 등을 사용하는 행위

응시자는 위에 언급된 사항의 부정행위 또는 위반을 인지하거나 이미 인지한 경우, 이를 준수할 책임이 있으며, 그러한 부정행위가 발생한 경우 응시자는 PECB 에 직접 보고하거나 발견한 즉시 PECB 에 알려야 합니다.

응시자는 PECB 시험 규칙 및 정책, 기밀유지 및 비공개 동의서, 윤리 강령을 이해하고 준수할 전적인 책임이 있습니다. 따라서 하나 이상의 규칙 위반이 확인된 경우 응시자는 환불을 받을 수 없습니다. 또한 PECB 는 채점 과정 중 또는 채점 후 부정행위가 확인된 경우 사안의 심각성에 따라 PECB 시험 응시 자격을 거부하거나 응시자에게 시험 재응시를 권유 할 수 있습니다.

위에 언급된 사항을 위반할 경우 PECB 는 금전적 보상으로도 만회 할 수 없는 막대한 손해를 입게됩니다. 따라서 PECB 는 시험 자료의 무단 공개 또는 오용을 시정하거나 방지하기 위해 즉각적인 금지 명령을 받는 것을 포함하여 적절한 조치를 취할 수 있습니다.

PECB 는 시험 규칙 및 정책을 위반하는 모든 이에 대해 PECB 시험 응시 영구금지, 기존 인증 취소 등의 조치를 취할 것입니다. 또한 PECB 의 저작권, 지적재산권, 기타 독점적 권리를 침해하는 개인 또는 기관에 대해 법적 조치를 취할 것입니다.

## 시험 결과

시험 결과는 이메일로 통보됩니다.

- 통보 기간은 시험일로부터 시작하여 에세이형 시험의 경우 3~8 주, 객관식 지필시험의 경우 2~4 주 동안 진행됩니다.
- 온라인 객관식 시험의 경우 결과를 즉시 받을 수 있습니다.

시험 합격자는 해당 인증제도의 인증 중 하나를 신청할 수 있습니다.

응시자가 시험에 불합격할 경우, 점수가 낮은 영역의 목록을 이메일에 추가하여 재응시 준비를 돕습니다.

시험 결과에 동의하지 않는 응시자는 결과를 받은 날로부터 30 일 이내에 이메일 ([examination.team@pecb.com](mailto:examination.team@pecb.com))로 재평가를 요청할 수 있습니다. 30 일 이후에 접수된 재평가 요청은 처리되지 않습니다. 응시자가 재평가 결과에 동의하지 않는 경우, 재평가 시험 결과를 받은 날로부터 30 일 이내에 [PECB 티켓팅 시스템](#)을 통해 민원을 제기할 수 있습니다. 30 일이 지난 후 접수된 불만 사항은 처리되지 않습니다.

## 시험 재응시 정책

시험 재응시 횟수에는 제한이 없습니다. 하지만 시험 응시일 사이에는 일정한 시간 간격이 준수되어야 합니다.

시험에 최초 응시했으나 불합격한 경우 응시일로부터 15 일이 경과한 후 재응시가 가능합니다(첫 번째 재응시).

**비고:** 파트너사 중 한 곳에서 교육 과정을 이수하고 첫 번째 시험에 불합격한 응시자는 쿠폰 코드를 받은 날로부터 12 개월 이내에 무료로 시험에 재응시 할 수 있습니다(첫 번째 시험 및 재시험 1 회는 강좌 수강료에 포함). 그렇지 않은 경우 재응시료가 부과됩니다.

재시험에서 불합격한 응시자의 경우, 다음 시험을 준비하기 위해 강좌를 수강할 것을 권장합니다.

교육 과정을 이수한 응시자가 시험 형식에 따라 재시험 일정을 잡으려면 다음 단계를 따라야 합니다:

1. 온라인 시험: 재시험 일정을 예약할때 최초 쿠폰 코드를 사용하여 수수료를 면제 받습니다
2. 지필 시험: 응시자는 재시험 일정(날짜, 시간, 장소, 비용)을 위해 처음 세션을 주최한 PECB 파트너/총판에게 연락해야 합니다.

파트너와 함께 교육 과정을 이수하지 않고 PECB 에서 직접 온라인 시험에 응시한 응시자는 이 정책의 적용을 받지 않습니다. 재시험 예약 절차는 최초 시험과 동일합니다.

## 제 3 장: 인증 프로세스 및 요구사항

### PECB ISO/ IEC 27001 자격 증명

PECB 자격인증을 위해서는 교육 및 실무경력에 관한 요구사항을 충족해야 합니다. 자신에게 적합한 자격증을 결정하려면 직무상 요건을 파악하고 인증 기준을 분석해야 합니다.

PECB ISO/IEC 27001 제도는 다음과 같은 요구사항이 있습니다:

자격 증명	교육	시험	실무 경력	MS 심사/사정 경력	기타 요구사항
PECB 인증 ISO/IEC 27001 심사원보(Provisional Auditor)	중등 교육 이상	PECB 인증 ISO/IEC 27001 선임심사원 시험(또는 이에 상당하는 시험)	없음	없음	<a href="#">PECB 윤리규정 서명</a>
PECB 인증 ISO/IEC 27001 심사원			2년: 정보보호경영 업무 경력 1년 포함	심사 활동: 총 200 시간	
PECB 인증 ISO/IEC 27001 선임심사원			5년: 정보보호경영 업무 경력 2년 포함	심사 활동: 총 300 시간	
PECB 인증 ISO/IEC 27001 시니어 선임심사원(Senior Lead Auditor)			10년: 정보보호경영 업무 경력 7년 포함	심사 활동: 총 1,000 시간	

유효성을 인정 받으려면, 심사 활동은 다음을 포함한 우수 심사 관행을 따라야 합니다.

1. 심사 계획
2. 심사 프로그램 관리
3. 심사보고서 작성
4. 부적합 보고서 작성
5. 심사 업무 문서 작성
6. 심사관련 문서화된 정보의 검토 및 관리
7. 현장심사 수행
8. 부적합 후속조치

## 9. 심사팀 인솔

### 자격인증 신청

시험 합격자(PECB 에 의해 인정되는 다른 시험 합격자 포함)는 자신이 응시한 PECB 자격증을 신청할 수 있습니다. PECB 자격인증을 받기 위해서는 특정한 교육 및 경력 요건을 충족해야 합니다. 자격인증 신청자는 온라인 자격인증 신청서를 작성해야 하며, 여기에는 자격인증 신청자의 전문 경력을 검증하기 위해 연락할 사람의 연락처 정보가 포함되어 있습니다(PECB 계정을 통해 액세스 가능). 자격인증 신청자는 영어, 프랑스어, 독일어, 스페인어 또는 한국어로 신청서를 제출 할 수 있습니다. 자격인증 신청자는 온라인으로 비용을 지불하거나 청구서를 요청할 수 있습니다. 자세한 내용은 다음을 참조하세요 [certification.team@pecb.com](mailto:certification.team@pecb.com).

온라인 인증 신청 프로세스는 매우 간단하며 다음의 절차에 따라 몇 분 안에 완료할 수 있습니다:

- 계정 [등록](#)
- 메일에서 확인 링크 확인
- [로그인](#)하고 자격인증 신청

자격인증 신청에 관한 더 자세한 정보는 [여기](#)를 참조하세요.

인증 담당부서는 신청자가 각 자격 증명과 관련된 모든 자격인증 요건을 충족하는지 확인합니다. 신청자는 자격인증 결정을 포함한 신청 상태에 대한 이메일을 받게됩니다.

인증 담당부서에서 신청서를 승인하면 신청자는 자격증을 다운로드하고 해당 디지털 배지를 신청할 수 있습니다. 자격증 다운로드에 대한 자세한 내용은 [여기](#)를 클릭하고, 디지털 배지 신청에 대한 자세한 내용은 [여기](#)를 클릭하세요.

PECB 는 영어 및 프랑스어로 지원을 제공합니다.

### 실무 경력

인증 신청자는 자신의 실무경력에 대해 모든 정보를 정확히 제공해야 합니다(직위, 업무 개시/종료일, 직무기술서 등). 또한 과거 진행했거나 현재 진행 중인 업무에 대해서도 충분한 상세정보와 함께 요약해 제출할 것을 권장합니다. 그 밖의 상세정보는 이력서에 포함할 수 있습니다.

## 프로페셔널의 추천(Professional References)

자격인증 발급 신청을 위해서는 1 건당 프로페셔널 2 명의 추천이 있어야 합니다. 프로페셔널은 프로페셔널 환경에서 자격인증 신청자와 함께 일한 바 있으며 신청자의 정보보호경영 경력과 현재 및 이전 업무 경력을 입증할 수 있어야 합니다. 자격인증 신청자의 감독을 받는 개인이나 친인척의 프로페셔널 추천은 유효하지 않습니다.

## ISMS 심사 경력

자격인증 신청자의 심사 로그를 확인해 필요한 심사 수행시간을 충족하는지 검증합니다. 사전 심사, 내부 심사, 제 2 자 심사 또는 제 3 자 심사 등의 심사 유형은 유효한 심사 유형으로 간주됩니다.

## 자격인증 신청 검토

인증 담당부서는 각 신청서를 검토하여 신청자의 자격인증 또는 자격증 프로그램에 대한 적격성을 검증합니다. 검토 진행 중에는 신청자에게 서면으로 통지가 이루어지며, 필요한 경우 추가서류를 제출할 수 있는 합리적 시한이 부여됩니다. 신청자가 마감시한까지 회신하지 않거나 주어진 시간 내에 필요한 서류를 제출하지 않을 경우, 인증 담당부서는 최초 제공된 정보만을 바탕으로 유효성을 검사하며, 이로 인해 신청자의 자격이 강등될 수 있습니다.

## 제 4 장: 자격인증 정책

---

### 자격인증 거부

PECB 는 다음의 경우 인증의 발급을 거절할 수 있습니다.

- 신청자가 신청서에 허위사항을 기재한 경우
- 신청자가 시험절차를 위반한 경우
- 신청자가 PECB 윤리규정을 위반한 경우

자격인증/자격증 프로그램이 거부된 신청자는 민원 및 항의 절차를 통해 이의를 제기할 수 있습니다. 자세한 정보는 ['민원 및 항의'](#) 장을 참고하세요.

자격인증/자격증 프로그램 신청 비용은 반환되지 않습니다.

### 자격인증 상태 옵션

#### 활성

자격인증 상태가 양호하고 유효하며, CPD 및 AMF 에 관한 PECB 요구사항을 충족하여 자격인증이 유지되고 있음을 의미합니다.

#### 효력정지

PECB 는 신청자가 요구사항을 충족하지 못할 경우 자격인증의 효력을 일시적으로 정지할 수 있습니다.

자격인증 효력정지의 기타 이유는 다음을 포함합니다.

- 관련자에 의해 과도한 민원 또는 심각한 민원이 제기된 경우(민원 내용에 대한 조사 완료시까지 효력정지)
- PECB 또는 인정기관의 로고가 의도적으로 오용된 경우
- PECB 가 제시한 기간 내에 인증마크의 오용을 바로잡지 않은 경우
- 자격인증 보유자 본인이 자발적으로 효력정지를 요청한 경우
- 기타 PECB 가 인증의 효력을 정지할 만한 상황으로 판단하는 경우

#### 자격인증 취소

PECB 는 자격인증 보유자가 PECB 의 요구사항을 충족하지 못할 경우 인증의 효력을 일시적으로 정지할 수 있습니다. 이러한 조치가 취해질 경우 대상자는 더 이상 PECB 인증 프로페셔널이라는 이력을 사용할 수 없습니다. 자격인증 취소의 추가 사유는 다음과 같습니다.

# PECB

- 신청자가 PECB 윤리규정을 위반한 경우
- 자격인증의 내용에 대해 부정확하거나 허위의 정보를 제공한 경우
- 기타 PECB 의 규칙을 위반한 경우
- 기타 PECB 가 적절하다고 판단하는 사유

자격인증이 취소된 신청자는 민원 및 항의 절차를 통해 민원을 제기할 수 있습니다. 자세한 정보는 [‘민원 및 항의’](#) 장을 참고하세요.

## 기타 상태

활성, 효력정지, 취소 상태 외에 인증을 자발적으로 철회하거나 명예인증으로 전환할 수 있습니다. 해당 상태와 영구 정지 상태에 대해 자세히 알아보려면 [인증 상태 옵션](#)으로 이동하세요.

## 자격인증 업그레이드 및 다운그레이드

### 자격인증 업그레이드

프로페셔널들은 요구사항을 충족한다는 것을 증명하는 즉시 자격인증을 업그레이드 할 수 있습니다.

업그레이드 신청을 하기 위하여 신청자는 PECB 계정에 로그인하여 "내 인증" 탭을 방문한 후 "업그레이드"를 클릭해야 합니다. 업그레이드 신청비는 \$100 입니다.

### 자격인증 다운그레이드

PECB 자격인증은 다음과 같은 이유로 더 낮은 자격증명으로 다운그레이드될 수 있습니다.

- 연간갱신비(AMF) 미납
- CPD 시간(크레딧)을 제출하지 않음
- 제출한 CPD 시간 불충분
- 요청한 CPD 시간에 대한 근거를 제출하지 않음

***비고:** 선임(lead) 자격인증을 보유한 PECB 인증 프로페셔널이 자격인증 갱신조건을 충족했다는 근거를 제공하지 못할 경우 인증이 다운그레이드됩니다. CPD 를 제출하지 않고 AMF 를 납부하지 않은 마스터 자격인증 보유자는 자격인증이 취소됩니다.*



## 자격인증 갱신

PECB 자격인증의 유효기간은 3 년입니다. PECB 인증 프로페셔널이 자격을 유지하려면 해당 자격증명과 관련된 요구사항을 충족해야 합니다(예: 필수 CPD 시간을 충족해야 함). 또한 연간갱신비 (\$120)를 지불해야 합니다. 자세한 정보는 PECB 웹사이트에서 다음을 참조하시기 바랍니다. [인증 유지](#)

## 자격인증 신청기간 만료

신청자가 1 년 이내에 자격인증 신청을 하지 않을 경우, 신청기간이 만료됩니다. 기간이 만료된 후 신청자는 새로운 신청기간을 시작할 수 있습니다. 그러나 PECB 는 만료 이전까지 적용 가능했던 조건, 표준, 정책, 수강생 핸드북에 대한 변동사항에 대한 책임을 지지 않습니다. 만료된 신청기간을 새로 시작하고자 하는 신청자는 서면으로 이메일 [certification.team@pecb.com](mailto:certification.team@pecb.com) 로 요청하고 요구되는 비용을 지불해야 합니다.

## 민원 및 항의 정책

민원은 자격인증여부 결정 후 30 일 이내에 제기해야 합니다. PECB 는 민원을 받은 후 30 영업일 이내에 신청자에게 서면으로 답변을 제공합니다. PECB 의 답변에 만족하지 못할 경우 민원 제기자는 항의를 제기할 권리가 있습니다.

민원 및 항의에 관한 자세한 정보는 [여기](#)를 참조하시기 바랍니다.

## 제 5 장: 일반정책

### 기타 인증기관이 공인하는 시험 및 자격인증

PECB 는 기타 인증기관이 공인하는 자격인증 및 시험을 인정합니다. PECB 는 동등성(equivalence) 프로세스를 통해 요청을 평가하여 해당 인증 혹은 시험이 PECB 인증과 동일하게 인정될 수 있는지 평가합니다(예: ISO/IEC 27001 선임심사원 인증).

### 차별금지 및 특수여건

모든 자격인증 신청은 나이, 성별, 인증, 종교, 국적, 혼인상태 등과 무관하게 객관적으로 검토됩니다.

자격을 갖춘 응시자 모두에게 공평한 기회를 보장하기 위해 PECB 는 필요한 경우 합리적인 여건<sup>2</sup>을 제공합니다. 응시자가 장애 혹은 특정 신체적 조건에 의해 특수한 여건을 필요로 하는 경우라면, 적절한 여건 조성을 위해 리셀러/총판에 통보해야 합니다<sup>3</sup>. 응시자가 장애/특별 요구사항과 관련하여 제공하는 모든 정보는 기밀로 취급됩니다. 장애인 응시자용 지원서를 다운받으려면 [여기](#)를 참조하시기 바랍니다.

### 행동 정책

PECB 는 총판, 파트너, 강사, 감독관, 시험출제자, 각종 위원회 및 자문위원회 위원, 고객(수강생, 시험응시자, 인증된 개인 및 자격증 보유자) 등 외부 이해관계자의 이익을 위해 최고 품질의 일관되고 접근 가능한 서비스를 제공할 뿐만 아니라 직원의 존엄성, 존중 및 인권을 존중하는 긍정적인 업무 환경을 조성 및 유지하는 것을 목표로 합니다.

이 정책의 목적은 PECB 가 당사 직원에 대한 외부 이해관계자의 용납할 수 없는 행동을 공평하고, 기밀이 유지되며, 공정하고, 적시에 관리하도록 보장하는 것입니다. 행동 정책에 관하여 더 자세히 보려면 [여기](#)를 클릭하세요.

<sup>2</sup> 미국 장애인법(ADA)에 따르면, '합리적 여건'이라는 용어는 다음을 포함할 수 있습니다: (A) 직원들이 사용하고 있는 기존 시설을 장애인이 사용할 수 있도록 준비, (B) 업무 조정, 파트타임 혹은 업무 스케줄 조정, 공식으로 전환 배정, 도구 혹은 기기 획득 또는 변경, 시험, 강좌 자료, 정책의 적합한 조정 혹은 조절, 자격을 갖춘 낭독자 혹은 통역사 제공, 기타 장애인을 위한 유사한 여건

<sup>3</sup> 2008 년 개정 ADA (P.L. 110-325) Sec. 12189. 시험 및 강좌 [제 309 장]: 신청, 라이선싱, 자격인증, 중등/고등교육, 프로페셔널, 무역 목적과 관련된 시험 또는 강좌를 제공하는 자는 장애인이 이용할 수 있는 장소와 방식으로 해당 시험 혹은 강좌를 제공하거나 장애인을 위한 별도의 조치를 취해야 한다.

## 환불 정책

환불 정책의 요구사항을 충족하는 경우 PECB 는 결제 금액을 환불해 드립니다. 환불정책을 확인하려면

[여기](#)를 클릭하세요.



**주소:**

본사  
6683 Jean Talon E,  
Suite 336 Montreal,  
H1S 0A5, QC,  
캐나다



**Tel./Fax.**

T: +1-844-426-7322  
F: +1-844-329-7322



**이메일:**

시험:  
[examination.team@pecb.com](mailto:examination.team@pecb.com)

인증:  
[certification.team@pecb.com](mailto:certification.team@pecb.com)

고객서비스:  
[support@pecb.com](mailto:support@pecb.com)



**PECB 헬프센터**

헬프센터에서 자주 묻는  
질문(FAQ)을 통해 PECB 웹사이트  
및 신청서 사용 관련 매뉴얼, PECB  
프로세스 관련 문서를 참조하거나  
지원센터의 온라인 추적 시스템을  
통해 연락하시기 바랍니다.

[www.pecb.com](http://www.pecb.com)