PECB BEYOND RECOGNITION

수강생 핸드북

ISO/IEC 27001 선임실무자

PECB

목차

제 1 장: 서론

PECB 소개

PECB 는 ISO/IEC 17024 에 따라 다양한 분야에서 개인에 대한 교육 및 인증 서비스를 제공하는 인증기관입니다.

PECB 는 국제적으로 인정되는 표준에 따라 가치 있는 서비스를 제공함으로써 프로페셔널들이 원칙을 준수하며 역량을 보유하고 있음을 증명하도록 지원합니다. PECB 의 미션은 신뢰를 강화하고, 지속적 개선을 촉진하며, 인증을 증명함으로써 사회 전체에 기여하는 것입니다.

PECB 의 주요 목적은 다음과 같습니다.

1. 프로페셔널의 인증에 필요한 최소요건 설정
2. PECB 인증 평가를 받을 자격이 있는지 확인하기 위해 신청자의 경력 검토 및 검증
3. 신뢰성을 갖춘 인증 평가방법 개발 및 유지
4. 요건을 충족하는 신청자에 대한 인증 발급, 기록 유지, 유효한 인증 보유자의 명단 공개
5. 주기적 인증 갱신의 요건 설정 및 해당 요건의 준수 보장
6. 신청자가 업무에 있어 윤리적 기준을 충족하도록 보장
7. 공통의 이해관계가 있을 경우 필요에 따라 PECB 네트워크의 멤버들을 대표
8. 다양한 분야의 기관, 기업, 공무원, 실무자 및 일반 대중에게 인증의 이점 홍보

PECB 인증의 가치

PECB 를 인증기관으로 선택해야 하는 이유

전 세계적 인지도

PECB 인증은 IAS(International Accreditation Service)로부터 국제적인 인정을 받고 공인되었습니다. PECB 는 국제인정협력기구(International Accreditation Forum) 다자간상호인정협정(Multilateral Recognition Arrangement)에 가입되어 있으며 이는 MLA 가입기관 간의 상호 인증을 보장하고 공인된 인증이 다양한 시장에서 승인될 수 있도록 합니다. 이처럼 국내는 물론 국제적으로 널리 인정되는 PECB 인증은 보유자에게 큰 도움이 됩니다.

임직원의 역량

PECB 의 핵심부서는 관련 분야의 경험을 지닌 역량 있는 임직원으로 구성되어 있습니다.
모든 임직원은 프로페셔널 인증을 보유하고 있으며, 고객만족 이상의 목표를 달성하기 위해 지속적인 교육을 받고 있습니다.

표준 준수

PECB 의 인증은 ISO/IEC 17024 를 준수하고 있다는 것을 증명합니다. 인증은 표준의 요건이 충분한 일관성, 프로페셔널리즘, 공정성을 바탕으로 충족 및 검증되었다는 의미입니다.

고객서비스

PECB 는 고객중심 기업으로, 모든 고객을 가치 있고 소중하게, 또한 프로페셔널하고 정직하게 대합니다.
PECB 는 고객 요청, 문제, 우려사항, 요구, 의견 지원을 전담하는 전문팀을 보유하고 있습니다. PECB 는 서비스의 품질을 유지하는 선에서 최대 24 시간 이내에 대응하고자 최선을 다하고 있습니다.

PECB 윤리강령(Code of Ethics)

PECB 프로페셔널은 다음을 준수합니다.

1. 정직, 정확, 공정, 책임, 자율을 바탕으로 프로페셔널하게 행동합니다.
2. 프로페셔널의 표준과 테크닉에 따라 전문 서비스를 제공함으로써 고용주, 고객, 대중, 자신의 직업에 가장 큰 이익을 제공하기 위해 노력합니다.
3. 각자의 분야에서 좋은 수준의 능력을 유지하고 프로페셔널 역량을 지속적으로 개선하기 위해 노력합니다.
4. 자신이 수행할 자격을 갖춘 전문 서비스만 제공하며, 고객에게 서비스와 관련된 우려사항이나 리스크, 서비스의 기타 성격에 대해 충분한 정보를 제공합니다.
5. 자신의 판단력에 영향을 미치거나 공정성을 해할 수 있는 사업상의 이해관계나 제휴관계에 대해 고용주나 고객에게 알립니다.
6. 현재 또는 과거의 고용주나 고객과의 사업상 관계에서 취득한 정보는 비밀로 취급합니다.
7. 전문 서비스 활동이 수행되는 지역의 모든 법률 및 규정을 준수합니다.
8. 타인의 지적재산과 기여를 존중합니다.
9. 프로페셔널 인증 신청자에 대한 평가 프로세스의 무결성을 해칠 수 있는 허위 또는 왜곡된 정보를 고의적으로 전달하지 않습니다.
10. PECB 또는 PECB 인증프로그램의 명성에 피해를 입힐 수 있는 어떤 태도로도 행동하지 않습니다.
11. 윤리강령 위반 혐의에 대한 조사에 성실히 협조합니다.

PECB 윤리강령 전문은 여기에서 다운로드 가능합니다.

ISO/IEC 27001 선임실무자 소개

ISO/IEC 27001 은 정보보안 관리시스템(ISMS)의 수립, 실행, 유지, 지속적 개선에 필요한 요구사항을 규정합니다. 시장에서 요구하는 가장 중요한 스킬은 ISMS 를 효과적으로 실행 및 관리하고 정보보안 리스크를 사정 및 처리하며 ISMS 실행 팀을 관리(혹은 참여)하는 것입니다.

'ISO/IEC 27001 선임실무자' 인증은 정보보안 관리시스템을 실행하고 ISMS 실행 팀을 주도할 수 있는 역량을 증명하고자 하는 개인을 위한 프로페셔널 인증입니다.

실행 담당자에 대해 가장 수요가 많다는 점으로 미루어 보았을 때, 국제적 인정을 받은 인증을 통해 커리어 잠재력을 충분히 발휘하고 프로페셔널 목표를 달성할 수 있을 것입니다.

PECB 인증은 라이센스나 단순 멤버십이 아니라는 점을 이해하는 것이 중요합니다. PECB 인증은 개인이 일련의 역량에 대한 능력과 이해를 증명했다는 점을 나타내는 동료 인정(peer recognition)입니다. PECB 인증은 신청자가 인증 분야에서의 경험을 입증하고 표준화된 시험을 통과했을 경우 수여됩니다.

본 문서는 ISO/IEC 17024:2012 를 준수하는 PECB ISO/IEC 27001 선임실무자(Lead Implementer) 인증제도를 명시하고 있습니다. 본 수강생 핸드북은 수강생이 인증을 취득 및 유지하는 프로세스에 관한 정보도 포함하고 있습니다. 신청서를 작성 및 제출하기 전에 반드시 본 수강생 핸드북의 모든 내용을 읽어보시기 바랍니다. 문의사항이 있을 경우 PECB 국제사무소로 연락주시기 바랍니다. certification.team@pecb.com.

PECB

제 2 장: PECB 인증 프로세스 및 시험 준비, 규칙, 정책

자신에게 적합한 인증 찾기

PECB 인증을 위해서는 교육 및 실무경력에 관한 요구사항을 충족해야 합니다. 어떤 인증이 적합한지 판단하기 위해서는 다양한 인증의 자격요건과 자신의 커리어에 무엇이 필요한지를 모두 검토해야 합니다.

시험준비 및 일정 등록

모든 응시자는 자신의 학습 및 인증시험 준비에 있어 스스로 책임을 져야 합니다. 인증 프로세스에서 특정 강좌나 학습커리큘럼 이수가 의무사항은 아닙니다. 그러나 강좌에 참여하면 응시자가 PECB 시험을 성공적으로 통과할 확률이 상당히 높아집니다.

시험 일정을 등록하는 방법은 다음과 같습니다.

1. 강좌와 시험을 제공하는 리셀러에게 연락을 취합니다. 특정 지역의 강좌 제공자를 찾기 위해서는 활동 중인 리셀러를 확인하시기 바랍니다. PECB 강좌 일정은 강좌 이벤트에서 확인하시기 바랍니다.
2. PECB 시험을 자택 혹은 기타 장소에서 원격으로 응시하고자 하는 개인은 시험 이벤트를 통해 PECB 시험 애플리케이션을 참조하시기 바랍니다.

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

시험 및 인증 신청 비용

PECB 시험은 강좌를 수강하지 않아도 응시할 수 있습니다. 비용은 다음과 같습니다.

- 선임(Lead) 인증시험: $1000
- 관리자(Manager) 인증시험: $700
- 기본(Foundation) 및 전환(Transition) 인증시험: $500

인증 신청비는 미화 500 달러입니다.

강좌를 수강하고 PECB 리셀러의 시험을 응시한 수강생의 경우, 신청비에는 시험, 인증 신청, 첫 해 연간갱신비(Annual Maintenance Fee, AMF)가 포함됩니다.

역량 영역

'PECB ISO/IEC 27001 선임실무자(Lead Implementer)' 시험의 목표는 조직이 정보보안 관리시스템(ISMS)을 효과적으로 계획, 실행, 관리, 모니터링, 유지하도록 지원할 수 있는 지식을 습득했는지 확인하는 것입니다.

ISO/ ISO 27001 선임실무자 인증은 다음과 같은 개인에게 적합합니다.

- 조직 내에서 정보보안 관리시스템의 실행에 관여하거나 관련이 있는 관리자 혹은 컨설턴트
- 조직 내에서 정보보안 관리시스템의 요구사항 준수 유지를 담당하는 개인
- ISMS 실행 팀의 구성원

시험에서는 다음과 같은 역량 영역을 평가합니다.

- **영역 1:** ISMS 의 기본 원칙과 개념
- **영역 2:** 정보보안 관리시스템(ISMS)
- **영역 3:** ISO/IEC 27001 을 바탕으로 ISMS 실행 계획하기
- **영역 4:** ISO/IEC 27001 을 바탕으로 ISMS 실행하기
- **영역 5:** ISO/IEC 27001 을 바탕으로 ISMS 모니터링 및 측정하기
- **영역 6:** ISO/IEC 27001 을 바탕으로 ISMS 를 지속적으로 개선
- **영역 7:** ISMS 인증심사 준비

영역 1: ISMS 의 기본 원칙과 개념 **주요 목표:** ISO/IEC 27001 원칙 및 개념을 이해하고 해석할 수 있다.	
역량	**지식**
1. 정보보안의 주요 개념을 이해 및 설명하는 능력 2. 정보, 자산의 차이점 및 관계를 설명하는 능력 3. 문서, 규격, 기록의 차이점을 이해하는 능력 4. 취약점, 위협, 리스크, 영향(impact)의 개념 간 관계를 이해하는 능력 5. 정보의 기밀성(Confidentiality), 무결성(integrity), 가용성(availability) 개념을 이해하는 능력 6. 보안 컨트롤의 분류와 목표를 이해 및 해석하는 능력 7. 자산, 리스크, 위협, 취약점, 컨트롤 사이의 관계를 이해하는 능력	1. 조직이 준수해야 하는 정보보안 법, 규정, 국제 및 산업 기준, 계약, 시장 관행, 내부 정책, 우수관행 등에 관한 지식 2. ISO/IEC 27001 의 주요 개념 및 용어에 관한 지식 3. 정보보안 리스크와 그것이 ISMS 에서 지니는 중요성에 관한 지식 4. 정보의 기밀성, 무결성, 가용성에 관한 지식 5. 정보보안 취약점, 위협, 리스크에 관한 지식 6. 보안 목표들의 차이점 및 특징에 관한 지식 7. 보안 컨트롤 종류 및 기능의 차이점에 관한 지식

영역 2: 정보보안 관리시스템(ISMS)

주요 목표: ISO/IEC 27001 부속서 A 에 나열된 보안 컨트롤을 이해하고 실행할 수 있다.

역량	지식
1. 정보보안 컨트롤을 선택, 설계, 설명하는 능력 2. 조직의 보안 아키텍처를 정의하는 능력 3. 정보시스템을 개발 및 사용하는 데 필요한 활동을 식별하고 설명하는 능력 4. ISO/IEC 27001 부속서 A 의 컨트롤을 이해, 해석, 분석하는 능력 5. ISO/IEC 27001 및 우수관행을 기반으로 부속서 A 컨트롤을 실행하는 능력	1. 액세스 컨트롤 서비스, 무결성 서비스, 암호화 서비스 등의 일반 보안 서비스에 관한 지식 2. 일반 아키텍처 프레임워크에 관한 지식 3. ISO/IEC 27001 부속서 A 컨트롤에 관한 지식

영역 3: ISO/IEC 27001 을 바탕으로 ISMS 실행 계획하기

주요 목표: ISO/IEC 29001 을 바탕으로 ISMS 실행을 계획할 수 있다.

역량	지식
1. ISMS 실행을 계획하기 위해 필요한 정보를 수집, 분석, 해석하는 능력	1. 프로젝트 관리의 주요 개념, 용어, 프로세스, 우수관행에 관한 지식
2. 정보보안 및 ISMS 목표를 이해하고 설정하는 능력	2. ISMS 실행에 사용되는 주요 접근법 및 방법론에 관한 지식
3. ISMS 리스크 및 그 영향(impact)을 식별하고 해석하는 능력	3. 일반적인 정보보안 및 ISMS 목표와 구체적인 결과를 달성하는 방법에 관한 지식
4. 조직의 내부 및 외부 상황을 분석하고 고려하는 능력	4. 조직의 내부 및 외부 상황의 일반적 구성요소에 관한 지식
5. ISMS 실행에 필요한 자원을 식별하는 능력	5. 조직의 상황을 이해하기 위해 사용되는 접근법에 관한 지식
6. ISMS 실행에 필요한 자원을 관리, 측정, 모니터링하는 능력	6. 조직에 대한 정보를 수집하고 관리시스템의 갭 분석을 수행하는 데 사용되는 테크닉에 관한 지식
7. ISMS 실행/운영 중 및 이후에 핵심 이해당사자의 역할과 책임을 식별하는 능력	7. ISMS 프로젝트 계획 및 ISMS 프로젝트 팀에 관한 지식
8. ISMS 프로젝트 계획을 작성, 정리, 검토하는 능력	8. ISMS 실행에 필요한 자원에 관한 지식
9. 갭 분석을 실행하고 정보보안 관리 목표를 명확히 하는 능력	9. 조직이 ISMS 를 관리하는 데 적합한 주요 조직 구조에 관한 지식
10. 조직의 구체적인 정보보안 목표에 적용된 ISMS 범위를 정의하고 그 근거를 설명하는 능력	10. 조직적, 기술적, 물리적 경계선 관점에서 ISMS 범위의 특징에 관한 지식
11. ISMS 정책을 개발 및 수립하는 능력	11. 정보보안 정책 및 절차를 작성하고 수립하는 데 사용되는 우수관행 및 테크닉에 관한 지식
12. 리스크 사정 프로세스의 다양한 단계를 수행하는 능력	12. 리스크 사정 프로세스 실행에 사용되는 다양한 접근법 및 방법론에 관한 지식
13. 적용성 보고서를 이해하고 작성하는 능력	13. 적용성 보고서의 특징에 관한 지식

영역 4: ISO/IEC 27001 을 바탕으로 ISMS 실행하기

주요 목표: ISO/IEC 27001 의 요구사항을 바탕으로 ISMS 를 실행할 수 있다.

역량	지식
1. 성공적인 ISMS 실행을 위한 역량 구축 프로세스를 관리하는 능력 2. ISMS 실행 및 운영을 지원하는 데 필요한 문서화 및 기록 관리 프로세스를 정의하는 능력 3. ISMS 운영에 필요한 프로세스를 정의, 설계, 실행하고 제대로 문서화하는 능력 4. 조직적 지식을 이해, 관리, 평가하는 능력 5. 빅데이터, 인공지능, 머신러닝, 클라우드 컴퓨팅, 업무 아웃소싱 등 오늘날의 세계 트렌드와 기술을 이해하는 능력 6. 적절한 정보보안 교육 및 인식제고 프로그램과 커뮤니케이션 계획을 정의하고 실행하는 능력 7. ISMS 커뮤니케이션 계획을 수립하여 조직의 정보보안 이슈, 정책, 성과에 대한 이해를 돕고 ISMS 성과를 개선하기 위해 인풋 혹은 제안을 제공하는 능력 8. 사고관리 정책 및 사고대응팀을 수립하는 능력 9. 비즈니스 연속성과 재해복구의 차이점을 이해하는 능력	1. 문서정보 라이프사이클 우수관행에 관한 지식 2. ISMS 정책, 절차, 가이드라인, 기준, 베이스라인, 워크시트 등과 관련된 다양한 문서정보의 특징 및 차이점에 관한 지식 3. 빅데이터의 '3V', 즉 데이터의 크기(volume), 다양성(variety), 속도(velocity)에 관한 지식 4. 약한 AI 와 강한 AI, 머신러닝에 관한 지식 5. IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service) 등의 클라우드 컴퓨팅 서비스에 관한 지식 6. 신기술이 정보보안에 미치는 영향에 관한 지식 7. 정보보안 교육 및 인식제고 프로그램과 커뮤니케이션 계획을 실행하는 특징과 우수관행에 관한 지식 8. 커뮤니케이션 이해당사자들의 지지와 신뢰를 증진하기 위한 커뮤니케이션 목표, 활동, 이해당사자에 관한 지식 9. 정보보안 우수관행을 바탕으로 한 사고관리 프로세스에 관한 지식 10. 비즈니스 연속성과 재해복구에 관한 지식

PECB

영역 5: ISO/IEC 27001 을 바탕으로 ISMS 모니터링 및 측정하기 **주요 목표:** ISMS 성과를 분석, 평가, 모니터링, 측정할 수 있다.	
역량	**지식**
1. ISMS 의 효과성을 모니터링 및 평가할 수 있는 능력 2. 식별된 ISMS 의 목표가 어느 정도 달성되었는지 검증하는 능력 3. ISMS 내부심사 프로그램을 정의 및 실행하는 능력 4. 조직의 정책 및 목표를 바탕으로 ISMS 의 적합성, 적절성, 효과성, 효율성을 보장하기 위한 정기적, 조직적 검토를 수행하는 능력 5. 경영진 검토 프로세스를 정의 및 수행하는 능력	1. ISMS 의 효과성을 모니터링 및 평가하는 데 사용되는 우수관행과 테크닉에 관한 지식 2. 측정 및 평가와 관련된 개념에 관한 지식 3. ISMS 내부심사 프로그램의 실행 및 운영과 관련된 주요 개념과 구성요소에 관한 지식 4. 중대한 부적합과 경미한 부적합의 차이에 관한 지식 5. 부적합 보고서 작성을 위한 가이드라인 및 우수관행에 관한 지식 6. 경영진 검토 수행에 사용되는 우수관행에 관한 지식

PECB

영역 6: ISO/IEC 27001 을 바탕으로 ISMS 를 지속적으로 개선하기 **주요 목표:** ISMS 의 지속적 개선에 대한 지침을 제공할 수 있다.	
역량	**지식**
1. 부적합을 추적하고 조치를 취하는 능력 2. 부적합의 원인을 식별 및 파악하고 이를 처리하기 위한 행동계획을 제안하는 능력 3. 조직이 ISMS 의 효과성 및 효율성을 지속적으로 개선하는 방법에 대해 조언할 수 있는 능력 4. 조직 내에 지속적 개선 프로세스를 실행하는 능력 5. 조직의 지속적 개선 프로세스를 지원하는 적합한 도구를 결정하는 능력	1. 부적합의 원인을 식별하는 데 사용되는 주요 프로세스, 도구, 테크닉에 관한 지식 2. 부적합 처리 프로세스에 관한 지식 3. 시정조치 계획을 개발하는 데 사용되는 주요 프로세스, 도구, 테크닉에 관한 지식 4. 지속적 개선과 관련된 주요 개념에 관한 지식 5. 변화 요인의 지속적 모니터링과 관련된 프로세스에 관한 지식 6. ISMS 유지 및 개선에 관한 지식

PECB

영역 7: ISMS 인증심사 준비

주요 목표: 조직이 ISO/IEC 27001 인증을 조직이 준비할 수 있도록 한다.

역량	지식
1. ISO/IEC 27001 인증 심사와 관련된 주요 단계, 프로세스, 활동을 이해하는 능력 2. ISMS 심사에서 근거기반 접근법을 이해, 설명, 명확히 할 수 있는 능력 3. 조직의 기대를 충족하는 인증기관을 식별 및 선택할 수 있도록 조언하는 능력 4. 조직이 ISO/IEC 27001 인증 심사를 받을 준비가 되었는지 판단하는 능력 5. 조직의 임직원이 ISO/IEC 27001 인증 심사 교육을 받고 준비할 수 있도록 하는 능력 6. 외부 심사원과 심사 결과 및 판단을 논의하고 이의를 제기할 수 있는 능력	1. 심사에 대한 근거기반 접근법에 관한 지식 2. 심사의 유형과 차이점에 관한 지식 3. 1 단계, 2 단계 심사의 차이점에 관한 지식 4. 1 단계 심사의 요구사항, 단계, 활동에 관한 지식 5. 문서정보 검토 기준에 관한 지식 6. 2 단계 심사의 요구사항, 단계, 활동에 관한 지식 7. 심사 후속조치, 단계, 활동에 관한 지식 8. 점검심사 및 재인증 심사의 요구사항, 단계, 활동에 관한 지식 9. ISO/IEC 27001 인증 심사 이후에 행동계획을 구성하기 위한 요구사항, 가이드라인, 우수관행에 관한 지식

위에 언급한 영역과 그 적합성에 따라 다음 표에 요약된 것과 같이 시험에 80 문항이 포함됩니다.

				요구되는 이해 수준(인지/분류)	
		역량 영역별 문항 수와 배점	역량 영역별 배점 비중(%)	이해, 적용, 분석을 측정하는 문항	종합 및 평가를 측정하는 문항
역량 영역	ISMS 의 기본 원칙과 개념	15	18.75	X	
	정보보안 관리시스템(ISMS)	12	15	X	
	ISO/IEC 27001 을 바탕으로 ISMS 실행 계획하기	18	22.5		X
	ISO/IEC 27001 을 바탕으로 ISMS 실행하기	14	17.5		X
	ISO/IEC 27001 을 바탕으로 ISMS 모니터링 및 측정하기	10	12.5	X	
	ISO/IEC 27001 을 바탕으로 ISMS 를 지속적으로 개선하기	6	7.5	X	
	ISMS 인증심사 준비하기	5	6.25		X
	합계	**80**	**100%**		
	이해 수준별 문항의 수			**43**	**37**
	각 이해 수준의 비중(인지/분류)			**53.75%**	**46.25%**

합격기준은 70% 입니다.

시험 합격 후, 응시자는 실무 경력에 따라 'PECB 인증 ISO/IEC 27001 선임실무자' 인증에 지원할 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 리셀러가 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 시험 형태에 관한 더욱 자세한 사항은 다음을 참조하시기 바랍니다. PECB 온라인 시험 가이드

본 시험은 객관식 문제를 포함합니다. 본 형식이 채택된 이유는 정의된 역량 영역과 관련된 학습 결과를 측정 및 평가하는 데 효과적이고 효율적인 방법임이 증명되었기 때문입니다. 객관식 시험을 통해 간단하고 복잡한 개념을 포함한 다양한 주제에 대한 응시자의 이해를 평가할 수 있습니다. 이러한 문제에 답할 때, 응시자는 다양한 원칙을 적용하고, 문제를 분석하며, 대안을 평가하고 다양한 개념 혹은 아이디어를 결합해야 합니다. 객관식 문제는 시나리오 기반이며 응시자는 시나리오를 읽고 해당 시나리오와 관련된 한 개 이상의 문제에 답해야 합니다. 본 객관식 시험은 문제가 맥락에 의존하기 때문에 '오픈북'으로 진행됩니다. 아래에 샘플 시험 문제가 있습니다.

시험이 '오픈북' 형태이기 때문에 응시자는 다음 참고 자료를 사용할 수 있습니다.

- 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 세션 중 답안을 베끼거나 공모하는 등 부정행위를 시도할 경우 자동으로 불합격 처리 됩니다.

PECB 시험은 영어 및 기타 언어로 제공됩니다. 특정 언어로 된 시험에 관한 문의는 다음으로 문의 바랍니다. examination.team@pecb.com.
참고: 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. 모든 PECB 객관식 시험에는 한 문제당 세 개의 선택지가 있으며, 정답은 하나입니다.

시험 유형, 제공 언어, 기타 세부사항은 다음을 참조하세요. PECB 시험 목록

시험 문제 샘플

시나리오:

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 정보보안 리스크 사정에 특히 집중하였다. 회사는 식별된 리스크를 평가할 목적으로 리스크 기준 또한 정의하였다.

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

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 정보보안 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 컨트롤이 실행되었는가?**
   A. 탐지 컨트롤
   B. **예방 컨트롤**
   C. 시정 컨트롤

4. **회사 A 는 리스크 사정 시 리스크 기준을 정의하였다. 이는 필요한 조치인가?**
   A. **예—회사는 정보보안 리스크를 사정할 때 리스크 기준을 수립 및 유지해야 한다.**
   B. 아니오—리스크 기준은 리스크 처리 옵션이 정의되었을 때만 수립되어야 한다.
   C. 아니오—리스크 기준은 정보보안 잔여 리스크가 수용되었을 때 수립된다.

시험결과 수신

시험 결과는 이메일로 통보됩니다. 결과는 합격 또는 불합격으로만 제공되며 점수는 포함되지 않습니다.

- 객관식 지필시험의 경우 결과 통보 기간은 시험일로부터 2 주~4 주입니다.
- 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 대비를 돕습니다.

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). 이때는 재응시료가 부과됩니다.
  참고: 강좌를 이수한 이후 지필시험에 응시해 불합격한 경우, 최초 응시일로부터 12 개월 이내에 무료로 1 회 재응시가 가능합니다.
- 시험에 2 번째로 응시했으나 불합격한 경우 응시일로부터 3 개월이 경과한 후 다음 응시가 가능합니다(2 번째 재응시). 이때는 재응시료가 부과됩니다.
  참고: 시험에 2 번째로 응시했으나 불합격한 응시자의 경우 다음 시험을 준비하기 위해 공식적인 강좌를 수강할 것을 권장합니다.
- 시험에 3 번째로 응시했으나 불합격한 경우 최초 응시일로부터 6 개월이 경과한 후 다음 응시가 가능합니다(3 번째 재응시). 이때는 재응시료가 부과됩니다.
- 4 번째 응시 이후에는 마지막 응시일로부터 12 개월이 지난 후에 다음 응시가 가능합니다. 이때는 재응시료가 부과됩니다.

시험 재응시와 관련한 사항(일자, 시간, 장소, 비용 등)은 최초 응시한 시험을 주관한 PECB 리셀러와 협의하시기 바랍니다.

시험 보안

프로페셔널 인증을 성공적으로 취득하는 과정에서 시험에 관한 보안과 기밀을 유지하는 것은 대단히 중요합니다. PECB 는 인증 보유자와 신청자가 PECB 시험의 보안과 기밀이 유지될 수 있도록 윤리를 준수할 것을 기대합니다. PECB 시험 내용의 정보를 공개하는 것은 PECB 윤리강령(Code of Ethics)의 위반으로 간주합니다. 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 일정 변경

시험 일자, 시간, 장소 혹은 기타 자세한 사항에 관한 문의는 다음으로 문의바랍니다.
examination.team@pecb.com

인증 신청

인증시험 합격자(PECB 에 의해 인정되는 다른 시험 합격자 포함)는 자신이 응시한 PECB 인증을 신청할 수 있습니다. PECB 인증을 받기 위해서는 특정한 교육 및 경력 요건을 충족해야 합니다. 인증을 신청하기 위해서는 인증 신청서 등(PECB 웹사이트에 등록된 자신의 계정에서 접속 가능)을 작성해야 합니다. 여기에는 신청자의 경력을 검증하기 위해 PECB 가 연락을 취할 참조인의 연락처가 포함되어야 합니다. 응시자는 신청서를 다양한 언어로 제출할 수 있습니다. 응시자는 온라인으로 비용을 지불하거나 청구서를 요청할 수 있습니다. 자세한 사항은 다음으로 문의바랍니다. 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
- 로그인하고 인증 신청

신청 절차에 관한 자세한 정보는 다음 링크에 있는 매뉴얼의 안내를 참고하시기 바랍니다. 인증신청

인증 부서가 신청자가 해당 인증의 요구사항을 모두 충족했다고 확인하면 신청서가 승인됩니다. 인증신청 결과는 신청자가 신청과정에서 기입한 이메일 주소로 통지됩니다. 신청이 승인된 경우, PECB 웹사이트에 등록된 자신의 계정에서 인증서를 다운로드할 수 있습니다.

PECB 는 영어 및 프랑스어로 지원을 제공합니다.

인증 갱신

PECB 인증의 유효기간은 3 년입니다. 인증을 갱신하기 위해서는 매년 자신이 해당 인증에 관한 업무를 수행하고 있음을 입증해야 합니다. PECB 인증 프로페셔널은 반드시 CPD(Continuing Professional Development) 크레딧을 매년 제출하고, 인증을 유지하기 위해 연간갱신비(AMF) $120 를 지불해야 합니다. 자세한 정보는 다음을 참조하시기 바랍니다. 인증 유지

인증 신청기간 만료

응시자가 3 년 이내에 인증 신청을 하지 않을 경우, 신청기간이 만료됩니다. 기간이 만료된 후 응시자는 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 응시자는 서면으로 요청하고 요구되는 비용을 지불해야 합니다.

제 3 장: 인증 요구사항

ISO/IEC 27001 선임실무자

PECB 의 ISO/IEC 27001 실무자 인증의 요구사항은 다음과 같습니다.

인증명	시험	실무경력	ISMS 프로젝트 경력	기타 요구사항
PECB 인증 ISO/IEC 27001 실무자보 (Provisional Implementer)	PECB 인증 ISO/IEC 27001 선임실무자 시험(또는 이에 상당하는 시험)	없음	없음	PECB 윤리규정 서명
PECB 인증 ISO/IEC 27001 실무자	PECB 인증 ISO/IEC 27001 선임실무자 시험(또는 이에 상당하는 시험)	2 년(정보보안 관리 경력 1 년 포함)	200 시간	PECB 윤리규정 서명
PECB 인증 ISO/IEC 27001 선임실무자	PECB 인증 ISO/IEC 27001 선임실무자 시험(또는 이에 상당하는 시험)	5 년(정보보안 관리 경력 2 년 포함)	300 시간	PECB 윤리규정 서명
PECB 인증 ISO/IEC 27001 시니어 선임실무자	PECB 인증 ISO/IEC 27001 선임실무자 시험(또는 이에 상당하는 시험)	10 년(정보보안 관리 경력 7 년 포함)	1,000 시간	PECB 윤리규정 서명

ISMS 프로젝트 경력이 인정되기 위해서는 프로젝트가 실행/관리 우수관행에 따라야 하며, 다음 활동이 포함되어야 합니다.

1. ISMS 실행 비즈니스 케이스 작성
2. ISMS 실행 프로젝트 관리
3. ISMS 실행
4. 문서정보 관리
5. 측정 실행
6. 시정조치 실행
7. 경영진 검토 수행

8. ISMS 성과 관리
9. ISMS 팀 관리

제 4 장: 인증규칙/정책

프로페셔널의 추천(Professional References)

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

실무경력

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.

ISMS 프로젝트 경력

인증 신청자의 ISMS 프로젝트 경력을 확인해 필요한 실무 수행시간을 충족하는지 검증합니다.

인증신청 검토

인증 담당부서는 신청자가 인증을 취득할 자격이 있는지 검증하기 위해 신청을 검토합니다. 검토 진행 중에는 신청자에게 서면으로 통지가 이루어지며, 필요한 경우 추가서류를 제출할 수 있는 합리적 시한이 부여됩니다. 신청자가 마감시한까지 회신하지 않거나 필요한 서류를 제출하지 않을 경우, 인증 담당부서는 최초 제공된 정보만을 바탕으로 신청을 검토합니다. 이로 인해 신청한 것보다 낮은 수준의 인증이 발급되거나 인증 자체가 부여되지 않을 수 있습니다.

인증발급 거절

PECB 는 다음의 경우 인증의 발급을 거절할 수 있습니다.

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

자세한 정보는 '민원 및 항의' 장을 참고하세요.

인증 신청비용은 반환되지 않습니다.

인증 효력정지

PECB 는 인증 보유자가 PECB 의 요구사항을 충족하지 못할 경우 인증의 효력을 일시적으로 정지할 수 있습니다. 인증 효력정지의 기타 이유는 다음을 포함합니다.

- 관련자에 의해 다수의 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
- 인증 보유자 본인이 자발적으로 효력정지를 요청한 경우
- 기타 PECB 가 인증의 효력을 정지할 만한 상황으로 판단하는 경우

인증 취소

PECB 는 인증 보유자가 PECB 의 요구사항을 충족하지 못할 경우 인증을 취소할 수 있습니다. 이러한 조치가 취해질 경우 대상자는 더 이상 PECB 인증 프로페셔널이라는 이력을 사용할 수 없습니다. 인증 취소의 기타 사유는 다음과 같습니다.

- 신청자가 PECB 윤리규정을 위반한 경우
- 인증의 내용에 대해 부정확하거나 허위의 정보를 제공한 경우
- 기타 PECB 의 규칙을 위반한 경우

인증 업그레이드

프로페셔널들은 요구사항을 충족할 경우 인증 업그레이드 신청을 할 수 있습니다.

업그레이드 신청을 하기 위하여 신청자는 PECB 계정에 로그인하여 '나의 인증' 탭에서 '업그레이드' 링크를 클릭하면 됩니다. 인증 업그레이드 신청비는 $100 입니다.

인증 다운그레이드

PECB 인증은 다음과 같은 이유로 더 낮은 인증으로 다운그레이드될 수 있습니다.

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

참고: 선임(lead) 인증을 보유한 PECB 인증 프로페셔널이 인증 갱신조건을 충족했다는 근거를 제공하지 못할 경우 인증이 다운그레이드됩니다. 마스터 인증을 보유한 PECB 인증 프로페셔널이 CPD 크레딧 보고와 연간갱신비 납부 의무를 충족하지 못할 경우 마스터 인증이 취소됩니다.

기타 상태

활성, 효력정지, 취소 상태 외에 인증을 자발적으로 철회하거나 명예인증으로 전환할 수 있습니다. 이러한 상태 및 영구정지, 신청 방법에 관한 자세한 정보는 다음을 참조하시기 바랍니다. 인증 상태

제 5 장: PECB 일반정책

PECB 윤리강령(Code of Ethics)

PECB 윤리강령 준수는 자발적 약속입니다. PECB 인증 프로페셔널은 윤리규정을 준수하고 다른 사람들도 이를 준수하도록 장려 및 지원하는 것이 중요합니다. 추가 정보는 여기를 참조하시기 바랍니다.

기타 시험 및 인증

PECB 는 기타 인증기관이 공인하는 인증 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 인증 신청은 나이, 성별, 인종, 종교, 국적, 혼인상태 등과 무관하게 객관적으로 검토됩니다.
자격을 갖춘 응시자 모두에게 공평한 기회를 보장하기 위해 PECB 는 필요한 경우 합리적인 여건을 제공합니다. 응시자가 장애 혹은 특정 신체적 조건에 의해 특수한 여건을 필요로 하는 경우라면, 적절한 여건 조성을 위해 리셀러/총판에 통보해야 합니다. 응시자가 제공하는 장애/요구 관련 정보는 철저히 기밀로 취급됩니다.

장애인 응시자용 지원서를 다운받으려면 여기를 참조하시기 바랍니다.

민원 및 항의

민원은 인증여부 결정 후 30 일 이내에 제기해야 합니다(시험 결정 포함). PECB 는 민원을 받은 후 30 영업일 이내에 응시자에게 서면으로 답변을 제공합니다. PECB 의 답변에 만족하지 못할 경우 민원 제기자는 항의를 제기할 수 있습니다. 민원 및 항의처리 절차에 관한 자세한 정보는 여기를 참조하시기 바랍니다.

(1) 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, 공석으로 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

(2) 2008 년 개정 ADA (P.L. 110-325). 총 12189 조 시험 및 강좌 [제 309 조]: 신청, 라이센싱, 인증, 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.