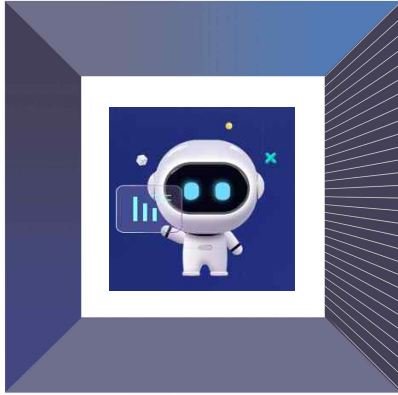


# 60 해외인증 실무 가이드북

## AI 인증제도 ISO/IEC 42001 & AI+



산업통상자원부  
해외인증지원단

KSA 한국표준협회

### 제품/서비스

품목명 (HS CODE)	AI 기술이 내장된 소프트웨어 산업용 로봇, AI 홈 로봇, 복합적인 AI 제품 8523.80.20, 8479.50, 8543.70 제품별 HSCODE	지역/국가	국제/모든국가
		인증명	ISO/IEC 42001 (인공지능경영시스템)
인증대상 기업유형	■ 기업유형 : AI 개발기업, AI 운영·서비스기업, AI 활용기업		
	유형	설명	
	AI 개발기업	AI 솔루션, 모델, 알고리즘을 설계·개발하는 기업	
	AI 운영·서비스기업	AI 플랫폼 운영자, AI SaaS 제공자, AI 데이터센터, AI 클라우드 운영조직	
	AI 활용기업	제조·의료·금융·유통 등에서 AI를 내부 의사결정 및 운영에 적용하는 조직	
인증대상 제품/서비스	■ 인증 대상 제품/서비스 : 좁은 의미의 특정 문제를 해결하기 위해 정의된 작업에 중점을 둔 인공지능 시스템의 유형에서 만 족스러운 수준의 성능으로 광범위한 작업을 처리하는 인공지능 시스템(AI) 유형까지를 포함.		
	구분	적용 가능 제품/서비스 (예시)	
	영상·보안	지능형 CCTV, 출입통제 AI 시스템, 지능형분석	
	제조·스마트 팩토리	예지정비, 품질검사 AI, 로봇비전	
	의료·헬스케어	AI 진단, 건강모니터링, 의료영상 분석	
	금융·신용	신용평가, 부정거래 탐지 AI	
	모빌리티	자율주행, 운전자 보조 AI 시스템	
	공공·행정	AI 민원분류, 의사결정 지원 시스템	
	언어·생성형 AI	챗봇, LLM API 플랫폼, 음성인식, 요약 서비스	
	교육·HR	AI 채용 평가, 학습 분석	
	에너지·스마트시티	AI 교통신호 제어, 에너지 수요예측	
	유사 키워드	인공지능 제품, 인공지능서비스, AI,	
마크	ISO/IEC 인증마크 표시는 획득한 인증 표준에 한해, 인증받은 범위 내에서, 인증기관 및 표준명 (예: ISO/IEC 42001)과 함께 명확히 사용해야 하며, 웹사이트, 광고 등 홍보물에 사용할 수 있으며, 제품이나 포장에는 사용할 수 없음. 마크는 인증기관의 지침에 따라 크기, 색상 등을 준수하여 사용해야 함.		

### 해외인증 실무가이드북 Part. 01 ISO/IEC 42001

### 인증개요

품목명 (HS CODE)	AI 기술이 내장된 소프트웨어 산업용 로봇, AI 홈 로봇, 복합적인 AI 제품 8523.80.20, 8479.50, 8543.70 제품별HSCODE	지역/국가	국제/모든 국가
인증마크		인증명 (제도명)	ISO/IEC 42001 (인공지능경영시스템)
인증유형	(유형1) <input type="checkbox"/> 제품인증 <input checked="" type="checkbox"/> 시스템	(유형2)	( <input type="checkbox"/> 강제 <input checked="" type="checkbox"/> 임의 <input type="checkbox"/> 기타)
인증 종류	<input checked="" type="checkbox"/> DoC <input checked="" type="checkbox"/> CoC ※ DoC(자기합성성 선언) / CoC(적합성 인증)		

### 인증소개

- 개요
- ISO/IEC 42001은 2023년 12월 국제표준화기구(ISO)와 국제전기기술위원회(IEC)가 공동 제정한 세계 최초의 인공지능(AI) 경영시스템 표준임. 이 표준은 조직이 인공지능 시스템을 책임 있게 개발 및 운영 그리고 관리하기 위한 체계적 관리 프레임워크를 제공하며, ISO 9001(품질경영시스템)이나 ISO/IEC 27001(정보보안경영시스템)처럼, AI분야의 "경영시스템 표준"임.
- 목적
- ISO/IEC 42001의 궁극적인 목적은 인공지능 기술의 신뢰성과 책임성을 확보하여 인간 중심의 안전하고 윤리적인 AI 생태계를 구축하는 데 있음.
  - 신뢰성과 투명성 확보
    - 인공지능 제품 및 서비스의 설계·개발·운영 전 과정에서 안전성, 공정성, 투명성, 설명 가능성 등 사회 신뢰를 확보하기 위한 관리 체계를 수립하도록 요구.
    - 이를 통해 AI의 오작동, 편향, 차별, 비윤리적 활용 등의 위험을 사전에 예방하고, 사용자와 이해관계자에게 신뢰할 수 있는 AI 서비스를 제공할 수 있음.

### Part. 01 ISO/IEC 42001



해외인증  
실무  
가이드북

## ISO/IEC 42001 인증소개

- 리스크 및 영향 관리의 체계화
  - 인공지능 제품 및 서비스를 제공할 때 조직, 개인, 사회에 미칠 수 있는 부정적 영향을 최소화하기 위해 위험 식별, 평가, 대응, 모니터링의 전 과정을 표준화된 절차로 관리할 수 있음.
  - 특히 데이터 품질, 모델의 공정성, 알고리즘의 보안성, 운영 과정의 오류 등 AI 특유의 리스크를 통합적으로 관리할 수 있는 프레임워크를 제공.
- 법적·윤리적 책임성 강화
  - ISO/IEC 42001은 EU AI Act, OECD AI 원칙, UNESCO 윤리 권고 등 국제 규범과 정합성을 이루며, 조직이 관련 법규 및 윤리 원칙을 준수할 수 있도록 지원함.
  - 이를 통해 AI 시스템이 인권을 존중하고, 차별 없는 사회적 가치 창출에 기여하도록 함.
- 지속적 개선 및 신뢰성 강화
  - 인공지능경영시스템은 PDCA(Plan-Do-Check-Act) 기반의 경영시스템 구조를 적용하여 인공지능 관련 프로세스를 지속적으로 점검·개선하도록 지원함.
  - 이 과정에서 조직은 성과 평가, 내부 심사, 경영 검토를 통해 AI 운영의 성숙도를 향상하고, 변화하는 기술·사회 환경에 신속히 대응할 수 있음.

## 글로벌 AI 인증 동향

- EU
  - EU AI Act는 기업의 고위험 AI 서비스에 대한 법적 준수 의무를 부여.
  - 검증된 국제 표준을 통해서 체계적인 이행을 검증받기 위해서 기업의 ISO/IEC 42001 인증 취득에 대한 니즈가 높음.
  - 통신업체, AI기술업체, IT업체를 중심으로 ISO/IEC 42001 인증을 획득.
  - ISO/IEC 42001은 EU AI Act의 추상적인 법률 조항에 대한 구체적인 AI 경영관리 프로세스와 통제 구조를 제시하고 있어 규제 준수를 위한 도구로 주목받고 있음.
- 미국
  - 미국 기업도 책임 있는 AI 기술 개발 및 서비스 운영에 대한 인증 및 규제 준수를 위하여 ISO/IEC 42001 도입을 추진하고 있음.
  - 주요 AI, IT 서비스 기업(Microsoft, AWS, Google 등)이 ISO/IEC 42001 인증을 취득하였음. 미국의 주요 기업은 특히 주요 클라우드 및 SaaS기업으로 B2B고객에게 책임있는 AI 서비스 개발 입증 및 경쟁 우위 확보를 하려는 전략에 기반함.

5

## AI 법령/규정

- 대한민국 AI 기본법: 2024.12 통과(추진체계, 인공지능 산업 육성 지원 및 고품향 인공지능에 대한 안전·신뢰 기반 조성), 2026.1.22 시행
- EU AI Act(Regulation (EU) 2024/1689): 세계 최초의 포괄적 AI 규정. 위험기반 접근(금지·고위험·제한적·최소 위험), GPAI(범용 AI) 의무, 제재(최대 글로벌 매출의 7%) 등을 규정.
- 미국 NIST AI RMF(NIST SP 800-37 Revision 2): 전 산업 인공지능 가이드(신뢰성 특성, 위험 식별/완화 프레임), 일부 주(e.g., 콜로라도주의 소비자보호에 관한 법(SB24-205), 캘리포니아주의 GenAI 학습데이터 투명성 법안(AB2013) 및 AI 투명성 법 (SB 942))에서 AI 관련 법률 제정 움직임
- 캐나다, AIDA(Artificial Intelligence and Data Act) 추진: 2022 제안, "이르면 2025년 이후" 시행 가능으로 안내했으나 2025-01 입법 추진이 중단되며 대안 모색 중(주·연방 다른 수단 병행).
- UNESCO AI 윤리 권고(2021), 194개 회원국 적용 가능한 글로벌 윤리 표준(투명성·책임성·인권 지속가능성 등 원칙).
- 사우디(SDAIA) AI 윤리 원칙(2023.9) 및 AI 채택 프레임워크(2024): 국내 모든 이해관계자 적용 지침
- OECD AI 원칙(2024) : GPAI 등 최신 이슈 반영. 가치 기반 원칙과 정책 권고 제공. 회원국 및 파트너 다수 채택.
- 일본(2025.3) : AI 사업자 가이드라인 v1.1 배포(AI 활용 사업자의 준수 사항을 제시)

## 관련표준

구분	표준명	주요내용
ISO/IEC 22989:2022	Artificial Intelligence — Concepts and terminology	인공지능의 기본 개념·용어 정의 (AIMS 용어 기준)
ISO/IEC 23053:2022	Framework for AI system using machine learning	머신러닝 기반 AI 시스템 프레임워크(데이터 모델 흐름)
ISO/IEC 23894:2023	Artificial Intelligence — Guidance on risk management	AI 특화 리스크 식별·평가 절차
ISO/IEC 42006:2025	AI Governance — Guidance for AIMS implementation	42001 실행 적용 가이드
ISO/IEC 38507:2022	Governance of IT — Governance implications of AI	경영진 차원의 AI 거버넌스 책임 가이드
ISO/IEC 5259 시리즈 (1-4)	Data quality for analytics and AI	데이터 품질 관리 기준 (정합성·완전성·정확성 등)
ISO/IEC 5338:2023	AI life cycle — Guidelines for AI system development	AI 수명주기 단계별 프로세스 가이드 (기획-데이터-개발-운영-폐기)
ISO/IEC 38500:2024	Governance of IT for the organization	조직의 IT 거버넌스 원칙 (책임·투명성 등)

6

## 인증기관

- 우리나라에서는 한국인증지원센터(KAB)가 경영시스템 인증기관 및 자격 인증기관에 대한 인정업무를 수행하고 있으며, IAF MLA 가입을 통해 국내 인증의 국제적 통용성을 보장하고 있음.
- 한국인증지원센터(KAB)에서 인증기관으로 승인받은 인증기관은 다음과 같음.

No.	기관명	주소	홈페이지	전화번호
1	한국표준협회	서울 강남	www.ksa.or.kr	02-6240-4662
2	(주)한국경영인증원	서울 영등포	www.ikar.co.kr	02-6309-9035
3	(주)케이에스알인증원	서울 금천	www.ksr-qes.com	02-858-2675
4	(주)에이씨티	경기 구리	www.acerti.co.kr	02-949-9553
5	한국생산성본부인증원(주)	서울 중구	www.kpcqa.or.kr	02-6973-9014

## 인증현황

- 2025년 11월 현재 KAB 인정 인증기관으로부터 ISO/IEC 42001 인증을 취득한 조직은 9개가 있으며, 인증 정보는 아래와 같음.
- 아래 인증 현황은 KAB 인증을 보유한 인증기관이 KAB가 운영하는 ISO 인증정보시스템(KAB CertiNet; KCN)을 통해 직접 입력한 정보이며 실제와 차이가 있을 수 있음.

No.	조직명	인증취득일	인증범위
1	S 사	2023년 12월	생활가전용 AI 시스템의 개발, 설계, 생산, 운용 및 서비스
2	L 사	2024년 1월	생활가전용 AI 시스템의 개발, 설계, 생산, 운용 및 서비스
3	K 사	2024년 1월	AI시스템을 활용한 금융 상품 및 금융 서비스
4	S 사	2024년 4월	AI 테크를 활용한 상품 및 서비스 개발, 운용
5	S 사	2024년 8월	AI기술을 적용한 B2B 상품/서비스의 개발, 운용 및 공급
6	I 사	2024년 9월	AI영상분석시스템(영상분석/산업안전/교통분석) 설계/개발 및 공급
7	N 사	2025년 4월	인공지능을 활용한 국제형 플랫폼 개발
8	L 사	2025년 6월	AI 기술을 활용한 통신/미디어 상품 및 서비스 개발, 운용
9	D 사	2025년 7월	AI기술을 적용한 B2B, B2C 서비스(AI Studios , Deepfake 탐지)의 개발, 운용 및 공급
10	T 사	2025년 11월	치연염 검출 시스템 Denti-HI 설계 및 개발
11	N 사	2025년 12월	암빅데이터센터(국가암빅데이터센터) 운영
12	S 사	2024년 9월	AI기반 종합솔루션(솔루어)의 개발 및 공급, 유지보수
13	D 사	2024년 12월	AI기반 솔루션의 개발 및 유지보수
14	M 사	2025년 3월	인공지능 기반 수임식물 위험예측 및 전자심사(SAFE-i24) 서비스
15	P 사	2025년 8월	반도체 설계 성능 진단 AI 플랫폼 사용
16	G 사	2025년 9월	생성형 AI 기반 Agent 플랫폼 운영 및 서비스

7

## 인증대상 제품/서비스

### □ 인증 대상기업 유형

- 인증 대상 기업 : AI 개발기업, AI 운영·서비스기업, AI 활용기업으로 나눌 수 있으며 기업에 대한 설명은 다음과 같음.

기업유형	설명
AI 개발기업	AI 솔루션, 모델, 알고리즘을 설계·개발하는 기업
AI 운영·서비스기업	AI 플랫폼 운영자, AI SaaS 제공자, AI 데이터센터, AI 클라우드 운영조직
AI 활용기업	제조·의료·금융·유통 등에서 AI를 내부 의사결정 운영에 적용하는 조직

### □ ISO/IEC 42001 인증 대상 제품/서비스

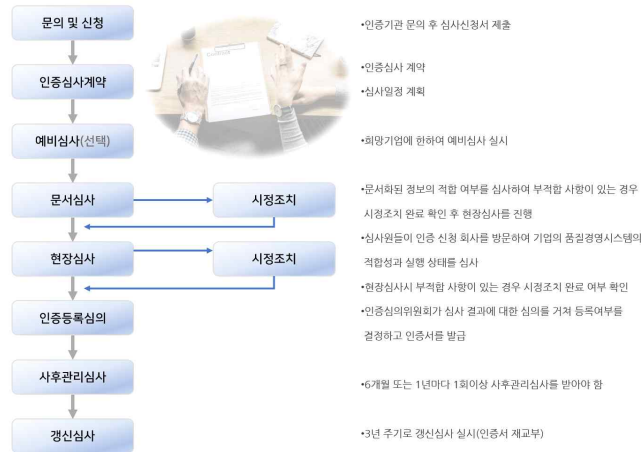
- 인공지능 제품/서비스는 좁은 의미의 어떤 특정 문제를 해결하기 위해 정의된 작업에 중점을 둔 인공지능 시스템의 유형에서 만족스러운 수준의 성능으로 광범위한 작업을 처리하는 인공지능 시스템 유형과 자를 포함하고 있음.

분야	제품/서비스(예시)
영상 보안	얼굴인식 CCTV, 출입통제 AI 시스템, 지능형 감시분석
제조 스마트팩토리	예지정비, 품질검사 AI, 로봇비전
의료 헬스케어	AI 진단, 건강모니터링, 의료영상 분석
금융 신용	신용평가, 부정거래 탐지 AI
모빌리티	자율주행, 운전자 보조 AI 시스템
공공 행정	AI 민원분류, 의사결정 지원 시스템
언어·생성형 AI	챗봇, LLM API 플랫폼, 음성인식, 텍스트 요약 서비스
교육·HR	AI 채용 평가, 학습 분석
에너지·스마트시티	AI 교통신호 제어, 에너지 수요예측
기타	머신러닝, 딥러닝을 활용한 제품/서비스

8

## 인증절차

- 인증 절차는 ① 인증기관 문의 → ② 인증심사 계약 → ③ (선택)예비심사 → ④ 1단계 심사(문서) → ⑤ 2단계 심사(현장) → ⑥ 인증 등록심의로 이루어집니다. 인증 획득 후에는 매년 1회 사후관리 심사를 받으며, 3년 주기로 갱신심사를 받아야 함.
- 기업에서 ISO/IEC 42001(인공지능경영시스템) 인증을 받는 절차를 기업 관점에서 쉽게 알 수 있도록 표현한 그림 (인증기관별 일부 다를 수 있음)



[그림 1-1] 인증 절차

## 인증신청

- 인증신청서는 인증기관별 양식을 사용해야 함.
- 일반적으로 신청서와 함께 기업 일반현황 및 AI 제품/서비스 설명자료 제출을 요구할 수 있음.
- 인증신청서 작성에 필요한 일반적인 사항과 작성 방법.
  - 조직정보
    - ① 기업명, 대표자, 담당자, 연락처 등으로 이루어져 있으며, 심사를 위하여 통역 가능 여부를 요구할 수 있음.
    - ② 인증신청 표준
      - \* 인공지능경영시스템 인증 신청 표준 : ISO/IEC 42001:2023.
    - ③ 인증신청 현황
      - \* 사업장 : 인증을 받고자 하는 사업장을 의미하며, 본사 또는 인증을 받고자 하는 사업장의 주소를 작성하고, AI 제품/서비스 개발, 공급, 활용을 지원하는 사업장이 별도로 있을 경우 지원사업장을 작성.
      - \* 인증신청 범위 : 인증을 받고자 하는 제품/서비스 도메인 또는 제품/서비스를 작성.
      - \* 인원수 : 인증 신청 사업장과 범위에 해당하는 인원을 작성.
    - ④ 업무 현황
      - \* 업무현황은 심사원에게 우리 회사가 어떤 일을 하는지, 인증 범위에 적합한 역량을 갖추었는지를 보여주는 중요한 부분으로 주요 사업 영역, 주요 AI 제품/서비스, 주요 핵심 기술, 주요 거래처 등의 내용을 작성.
      - \* 신청서 앞부분에 기재한 인증 신청 범위와 내용이 서로 어긋나지 않아야 함.
      - \* 도식화나 개조식을 활용할 수 있으며, 보유하고 있는 핵심 기술력과 인프라를 짧게 작성하는 것이 좋음.
    - ⑤ 업무 프로세스
      - \* 제품이나 서비스를 만들기 위해 어떤 단계를 거치는지, 그리고 각 단계가 어떻게 연결되는지를 보여 주는 것이 핵심입니다.
      - \* 글로 길게 쓰는 것보다 아래와 같은 흐름(Flow)을 텍스트로 표현해 주는 것이 심사원이 이해하기 가장 좋음.
      - \* 고객 요구사항 접수 → 계약 검토 → 개발 계획 수립 → 개발 및 개발관리 → 데이터 관리 → 성능/품질 검사 → 배포 → 사후 관리(A/S)
      - \* 업무 프로세스에 따른 관련 부서를 기록하는 것도 좋은 방법.

9

10

## 인증심사 문서

- 기업에서 인공지능경영시스템 인증을 위해 준비해야 할 문서와 기록을 구분하여 요약.
- "경영문서"는 인공지능경영을 위한 계획과 프로세스 관련 문서이고, "운영기록"은 프로세스에 따라 실행한 결과를 입증하는 자료.

### □ 경영문서

- 기업이 인공지능경영시스템을 체계적으로 운영하기 위해 수립·관리해야 하는 기본 정책 및 계획, 절차 등의 문서.
- 주요 경영 문서는 다음과 같음.
  - 인공지능경영시스템의 적용범위
  - AI 리스크 영향 평가 기준 및 처리 프로세스
  - 인공지능 수명주기 관리 프로세스
  - 데이터 관리 및 거버넌스 프로세스
  - 문서화된 정보 관리 체계
  - AI 방침, 목표, 내외부 이슈, 이해관계자 요구사항
  - 조직의 역할 책임-권한
  - 자원 및 역량 관련 문서(교육 인식-증명자료 등)
  - 적응성 보고서(Statement of Applicability)

### □ 운영기록

- 기업에서 인공지능경영시스템이 실제로 운영되고 있음을 입증하는 기록.
- 필수 기록은 다음과 같음.
  - AI 리스크 영향 평가 결과 기록
  - 운영계획 및 통제 수행기록 (개발, 배포, 운영, 유지보수 관련 실행 증거 포함)
  - 모니터링 및 측정(성능) 결과 기록
  - 내부심사 결과 및 시정조치 기록
  - 경영검토 보고서
  - AI 개발 데이터-운영-폐기 관련 각종 기록

## ISO/IEC 42001 핵심 준비사항

- 1~3절은 개요 및 용어 정의의 본 가이드에서 제외하였으며, 인증 표준의 핵심인 4~10절 "AI 시스템의 기획 운영 평가 개선"에 대한 경영시스템 프레임워크 중심으로 안내.
- ISO/IEC 42001은 조직이 신뢰성 안전성-공정성을 갖춘 AI를 책임 있게 관리하도록 요구사항이 구성됨.
- 조항과 핵심요구사항은 인증을 획득하고자 하는 기업이 체크리스트로 사용할 수 있도록 구성.

주요조항		핵심내용
4	조직의 상황	이해관계자, 내부 외부 이슈 파악
5	리더십	경영진의 책임, AI 방침 수립
6	기획	리스크 및 기회관리, AI 목표 설정
7	지원	자원, 역량, 의사소통, 문서화
8	운용	AI 리스크평가 처리, 영향평가
9	성과평가	내부심사, 경영검토
10	개선	지속적 개선, 부적합 및 시정조치

### 4절. 조직의 상황 핵심 준비사항

조항번호	조항명	핵심 준비사항
4.1	조직과 조직 상황 이해	AI 시스템 운영에 영향을 미치는 내부 외부 이슈를 결정해야 함 (기술, 법규, 사회적 가치, 윤리, 이해관계자 등)
4.2	이해관계자의 요구 및 기대 이해	사용자, 규제기관, 데이터 주체, 공급자 등 이해관계자의 요구사항 및 기대를 결정하여야 함
4.3	AIMS의 적용범위 결정	인증의 적용범위(scope)를 명확히 정의해야 함 (AI 시스템, 서비스, 관련 조직 단위 포함)
4.4	AI경영시스템	최고경영자는 AIMS의 효과성과 책임성 확보를 위해 리더십과 의지를 표명하고 실행해야 함

### 5절. 리더십 핵심 준비사항

조항번호	조항명	핵심 준비사항
5.1	리더십과 의지표명	조직의 전략적 방향과 연계한 AI방침과 시목표를 수립하고 자원의 가용성보장, 성과 달성, 지속적 개선에 대한 리더십과 의지표명을 해야 함
5.2	AI 방침	조직은 AI 원칙 가치-책임 윤리 기준을 포함한 공식적인 AI 방침을 수립하고, 조직내 의 사소통하고 이해관계자가 이용가능해야 함
5.3	조직의 역할-책임-권한	AIMS 구축 운영 감사에 대한 책임자와 권한(예: AI 책임자, 데이터 관리자) 을 명확히 정의해야 함

### 6절. 기획 핵심 준비사항

조항번호	조항명	핵심 준비사항
6.1	리스크 및 기회를 다루기 위한 조치	조직은 AI 시스템 관련 리스크(위험)와 기회를 식별하고, 관리 방안을 수립해야 함. (ISO 31000-23894 기반)
6.1.2	AI 리스크 평가	AI 데이터, 모델, 시스템, 사회적 측면 등 다차원적 리스크를 평가해야 함.
6.1.3	AI 리스크 처리	리스크 경감, 회피, 이전, 수용 등 여러 전략을 문서화해야 함.
6.1.4	AI 시스템영향 평가	개인 집단 사회에 미치는 AI 영향을 정성-정량적으로 평가해야 함.

조항번호	조항명	핵심 준비사항
6.2	AI 목표 및 달성계획	신뢰성, 투명성, 공정성 등 AI 목표 및 성과지표를 설정하고 측정 관리해야 함.
6.3	변경의 계획	AI 시스템, 데이터, 프로세스 변경 시 리스크 재평가 및 승인 절차를 수행해야 함.

#### 7절. 지원 핵심 준비사항

조항번호	조항명	핵심 준비사항
7.1	자원	AIMS 운영에 필요한 인적, 기술적, 데이터, 인프라 자원을 확보하고 관리해야 함.
7.2	역량	AI 관련 인력이 적절한 교육 훈련 경험을 보유해야 하며, 정기적 역량평가 실시.
7.3	인식	임직원은 AI 방침, 리스크, 윤리적 영향 등을 인식해야 함.
7.4	의사소통	내부 외부 이해관계자와의 AI 관련 의사소통 체계를 수립해야 함.
7.5	문서화된 정보	모든 정책, 절차, 데이터 기록 등을 식별 관리 보존해야 함 (버전, 승인, 변경관리 포함).

#### 8절. 운용 핵심 준비사항

조항번호	조항명	핵심 준비사항
8.1	운용 기획 및 통제	AI 시스템의 운영 전 과정에 대해 계획 절차 통제 활동을 수립해야 함.
8.2	AI 리스크 평가	6.1에서 정의된 리스크 관리 프로세스를 실제 운영단계에 적용.
8.3	AI 리스크 처리	리스크 저감 조치 실행 및 잔여리스크 문서화.
8.4	AI 시스템 영향 평가	AI 시스템이 개인 사회에 미칠 영향의 정기적 재평가 수행 (운영 중에도 지속 수행).

#### 9절. 성과평가 핵심 준비사항

조항번호	조항명	핵심 준비사항
9.1	모니터링 측정 분석 평가	AI 성능, 신뢰성, 윤리 준수, 리스크 대응 성과 등을 지속적으로 모니터링 및 평가해야 함.
9.2	내부심사	주기적으로 AIMS의 적합성과 효과성을 점검해야 함 (ISO 19011 기반).
9.3	경영검토	최고경영진은 AIMS 성과, 리스크, 개선기회를 정기적으로 검토해야 함.

#### 10절. 지속적 개선 핵심 준비사항

조항번호	조항명	핵심 준비사항
10.1	지속적 개선	AIMS의 성능을 개선하기 위해 지속적 개선 프로세스를 운영해야 함.
10.2	부적합 및 시정조치	AI 운영 중 발견된 부적합 사항을 조사 원인분석 사정조치하여 재발 방지해야 함.

13

### 인증 표시 사항

#### □ 인증 표시 사용

- ISO(국제표준화기구) 로고 사용 방법은 일반적인 제품 브랜드 로고와 달리 매우 엄격한 규정이 적용. 가장 중요한 점은 기업이 ISO 자체 로고를 직접 사용하는 것이 아니라, 인증기관으로부터 받은 '인증마크'를 사용해야 함.

#### □ ISO 표시 방법 및 규격

- 인증마크는 반드시 인증기관의 인증마크와 동시에 사용되어야 하며, 인정마크와 인증마크의 혼동을 피하기 위해 다음과 같이 인증마크를 우측 또는 하단에 위치하도록 배열함을 원칙으로 함.
- 인증마크는 원본을 확대·축소하여 사용할 수 있으나, 인정마크의 크기는 최소한 15mm 이상(가로 15mm, 세로 10mm)이 되어야 함.



[그림 1-2] 인증마크

#### □ 인증표시의 사용이 가능한 경우

- 광고 또는 홍보물 : 산업분류상 인증기업의 제품으로 분류되지 않는 명판, 명함 및 인증기관의 교재, 편지지, 브로셔, 문서, 송장, 인증서 및 수료증 등의 인쇄물 또는 제작물 또는 기타 광고수단.
- 문구는 인증된 클라이언트의 식별 정보 (예: 브랜드나 회사명), 경영시스템 유형 (예: 품질, 환경) 및 해당하는 표준, 인증서를 발행한 인증기관을 포함.

#### □ 인증표시의 사용이 제한되는 경우

- 제품 또는 제품포장 : 제품 유통을 위한 최소 단위의 품목과 담뱃갑, 통조림, 음료수 캔 등의 용기와 같이 제품 단독으로는 유통이 불가능한 단위포장.
- 거래 샘플 또는 기타 제품 적합성에 관한 진술서
- 깃발, 건물 또는 차량.
- 단, 상품의 포장 등에 인증표시를 하지 않고 'KSA로부터 KSA Q ISO 9001 인증을 획득한 시스템 하에서 제조된 ○○'라는 방식으로 표시.

14

### 인증 기간 및 비용 (KSA)

- 인증 비용 : ISO/IEC 42001 인증비용은 심사일수(투입 MD)와 심사 범위를 기반으로 산정되며, 일반적으로 아래 항목으로 구성 (심사일수·비용 산정을 위한 신청서 기반 운영 가능).
  - 신청/접수비(또는 계약·등록 관련 비용)
  - 심사비: 심사일수(MD) × 심사 단가
  - 출장비: 심사 수행에 필요한 교통·숙박 등(내규/기준 적용)
  - 심사단가 : 조직 규모에 따라 대기업 110만 원, 중견기업 95만 원, 소기업 75만 원 수준으로 적용되며,VAT 및 출장비는 별도 산정됨.

#### － 심사MD 기준표

*유효인원수	AI생산자	AI개발자/공급자	AI사용자	다중역할
1~10	5.0	3.5	3.5	6.5
11~15	6.0	4.0	4.0	8.0
16~25	7.0	4.5	4.5	9.5
26~45	8.5	6.0	6.0	11.5
46~65	10.0	7.0	7.0	13.0
66~85	11.0	7.5	7.5	15.0
86~125	12.0	8.0	8.0	16.0
126~175	13.0	9.0	9.0	17.5
176~275	14.0	9.5	9.5	19.0
276~425	15.0	10.0	10.0	20.0
425명 이상	위와같이 증가	위와같이 증가	위와같이 증가	ISO/IEC 42006 A.3.2참조

\* AI 수명주기 프로세스와 관련된 조직의 관리 하에 있는 인원수(ISO/IEC 42006, A.3.2참조)

### FAQ

<p><b>1) ISO/IEC 42001은 “AI 제품을 만드는 회사”만 해당되나요?</b></p> <p>아니요. AI 시스템을 개발·제공(공급자) 하든, 구매해 운영 활용(사용/배포자) 하든 모두 대상이 될 수 있습니다. 핵심은 “조직이 AI를 어떻게 관리하고 책임 있게 운영하는지”를 입증하는 것입니다.</p>
<p><b>2) 우리 회사는 AI가 일부 기능에만 들어가는데도 인증이 필요할까요?</b></p> <p>가능합니다. 인증 범위를 “AI가 들어간 제품/서비스/프로세스만”으로 좁혀서 적용범위(scope)를 설정 할 수 있어요. 다만 범위를 좁힐수록 ‘AIMS 설계, 제와 사유, 책임 범위’를 문서로 명확히 해야 심사에서 흔들리지 않습니다.</p>
<p><b>3) ISO/IEC 42001 인증을 받으면 인공지능기본법, EU AI Act도 자동으로 충족되나요?</b></p> <p>자동 충족은 아닙니다. 다만 ISO/IEC 42001은 관리체계(거버넌스·리스크 운영통제 개선)를 갖춰 체계 해워서 인공지능기본법과, EU AI Act 대응의 기반이 됩니다. 실무에선 ISO 42001(AIMS) + EU AI Act 기술문서/요건(투명성 로그·인간감독 등)을 매핑해서 같이 준비하는 경우가 많습니다.</p>
<p><b>4) ISO/IEC 27001(정보보호)과 같이 운영할 수 있나요?</b></p> <p>네, 맞습니다. ISO/IEC 42001도 ISO의 공통 구조(HLS)를 따르기 때문에 문서관리, 내부심사, 경영검토, 사정조치, 리스크 접근 같은 운영을 통합하기 좋아요. 팀: 공통 프로세스는 통합하고, AI 특화(리스크 영향평가 AI 목표 운영 모니터링)를 보강하십시오.</p>
<p><b>5) Annex A 통제는 “무조건 전부” 적용해야 하나요?</b></p> <p>보통 전부 강제는 아닙니다. 조직 상황에 맞게 통제를 채택/비채택하고, 그 근거와 적용 방식을 정리하는 것이 핵심입니다(실무에서는 SoA 성격 문서로 정리). 심사에서 자주 보는 포인트: “왜 뺐는지”, “대신 어떤 통제로 리스크를 관리하는지”</p>
<p><b>6) 가장 먼저 준비해야 하는 문서는 무엇인가요?</b></p> <p>우선순위를 이렇게 집으면 빠릅니다. 1. 적용범위(Scope) 2. AI 방침(Policy) &amp; 역할/책임(R&amp;R) 3. AI 리스크 평가/처리 프로세스 + 기록 양식 4. AI 영향평가 프로세스 + 결과 기록 5. 운영 모니터링(성능 편향 드리프트·보안 로그 등) 체계</p>

<p>7) "리스크 평가"와 "영향평가"는 어떻게 달라요?</p> <p>- 리스크 평가: 실패/오작동/보안사고/규제위반 등 발생 가능성과 피해 중심          - 영향평가: 개인정보, 차별, 인권, 안전, 이해관계자 피해 등 사회 인권 사용자 영향 중심          - 리스크와 영향평가를 한 시트로 운영해도 되지만, 판단 기준과 산출물(결과 기록)은 구분되는 게 좋습니다.</p>
<p>8) 모델카드/데이터카드/사용자 매뉴얼은 ISO/IEC 42001에서 필수인가요?</p> <p>모델카드/데이터카드/사용자 매뉴얼이 ISO/IEC 42001에서 요구하는 필수 문서는 아닙니다.          다만 실무적으로는 모델카드/데이터카드/사용자 매뉴얼이 가장 효율적인 증명이라 많이 채택합니다.          모델카드/데이터카드/사용자 매뉴얼은 심사에서 투명한 정보제공과 신뢰성에 매우 유용한 증빙 문서입니다.</p>
<p>9) 내부심사는 누가 해야 하나요? 외부인이 해야 하나요?</p> <p>내부심사는 내부 인력이 해도 됩니다.          다만 심사 대상 업무로부터 독립성/객관성이 확보되어야 합니다.          예를 들면 개발팀을 심사할 때는 개발팀이 아닌 품질/준법/보안이 심사하고, 품질팀은 개발팀이 심사하여 독립성/객관성을 확보합니다. 필요시 기술전문가를 배석시키는 방식도 좋은 방법입니다.</p>
<p>10) 인증심사(1단계/2단계)는 무엇을 보는 건가요?</p> <p>1단계(문서 및 준비상태 중심)는 인공지능경영시스템 문서가 갖춰졌는지, 핵심 프로세스가 설계됐는지 확인합니다. 2단계(현장 운영 중심)는 인공지능경영시스템이 실제로 돌아가는지(평가 수행, 운영기록, 모니터링, 개선/조정조치) 확인합니다. 2단계는 "문서"보다 기록(증거)을 중심으로 확인합니다.</p>

## 참고자료

- ISO/IEC 22989:2022 - Artificial Intelligence - Concepts and Terminology
- ISO/IEC 23894:2023 - Artificial Intelligence - Guidance on Risk Management
- ISO/IEC 23053:2022 - Framework for AI System Using Machine Learning
- ISO/IEC 5338:2023 - AI Life Cycle Processes - Guidelines for Development and Use
- ISO/IEC 5259 (Parts 1-4) - Data Quality for Analytics and AI
- ISO/IEC 38507:2022 - Governance of IT - Governance Implications of AI
- ISO/IEC TR 24368:2022 - Overview of Ethical and Societal Concerns of AI Systems
- ISO/IEC TR 24028:2020 - Trustworthiness in Artificial Intelligence - Overview of Key Concepts
- ISO 31000:2018 - Risk Management - Guidelines
- ISO 9001:2015 - Quality Management Systems - Requirements
- ISO/IEC 27001:2022 - Information Security Management Systems - Requirements
- ISO/IEC 27002:2022 - Code of Practice for Information Security Controls
- ISO/IEC 27701:2025 - Privacy Information Management System (PIMS)
- ISO 19011:2018 - Guidelines for Auditing Management Systems
- OECD AI Principles (2019, revised 2024)
- UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)
- EU AI Act (Regulation (EU) 2024/1689)
- NIST AI Risk Management Framework v1.0 (2023)
- Council of Europe Framework Convention on Artificial Intelligence (2024)
- G7 Hiroshima Process on Generative AI (2023)

## Part. 02 AI+ 인증

## 해외인증 실무 가이드북

## AI+ 인증소개

### 1. 인증개요

20

## 인증개요

<p>품목명 (HS CODE)</p>	<p>AI 기술이 적용된 모든 소프트웨어, 산업·홈 로봇, AI서비스 및 ICT 제품, AI 융복합 제품 8523.80.20, 8479.50, 8543.70 제품명 HSCODE</p>	<p>지역/국가</p>	<p>대한민국</p>
<p>인증마크</p>	<p>인증 마크 </p>	<p>인증명 (제도명)</p>	<p>AI+ (에이아이플러스)</p>
<p>인증유형</p>	<p>(유형1) <input checked="" type="checkbox"/> 제품인증 <input type="checkbox"/> 시스템</p>	<p>(유형2)</p>	<p>( <input type="checkbox"/> 강제 <input type="checkbox"/> 임의 <input checked="" type="checkbox"/> 기타)</p>
<p>인증종류</p>	<p><input type="checkbox"/> DoC <input checked="" type="checkbox"/> CoC ※ DoC(자기적합성 선언) / CoC(적합성 인증)</p>		

## 인증소개

### □ 개요

- AI+ 인증은 인공지능(AI) 기술이 적용된 제품·서비스의 품질, 신뢰성, 안전성을 객관적으로 검증하기 위한 국내 최초이자 세계 최초 수준의 AI 제품·서비스 인증 제도.
- 인공지능기본법 제정, ISO/IEC 42001:2023(인공지능 경영시스템), EU AI Act 시행 등 국내외 규제 이해관계자의 신뢰를 확보할 수 있도록 설계.

### □ 목적

- AI+ 인증은 인공지능 기술이 적용된 제품과 서비스가 신뢰할 수 있고 안전하게 활용될 수 있도록 품질과 성능, 운영체계를 객관적으로 검증하기 위한 인증제도.
- 이를 통해 기업은 강화되는 국내외 AI 규제에 선제적으로 대응하고, AI의 기획·개발·운영 전 과정에서 책임 있는 AI 관리 역량을 확보하며, 고객과 사회 전반에 검증된 AI에 대한 신뢰를 제공하는 것을 목적으로 함.
  - AI 품질 보증: AI 모델 성능, 소프트웨어 품질, 신뢰성·안전성에 대한 객관적 검증
  - 책임 있는 AI 구현: 기획부터 개발·운영·폐기까지 전 생애주기 관리체계 확인
  - 규제 선제 대응: EU AI Act, 한국 AI 기본법 등 국내외 AI 규제 대응 근거 확보
  - 대외 신뢰성 강화: 고객, 파트너, 투자자, 공공기관을 대상으로 한 신뢰 마크 제공



## AI 제품/서비스 인증 동향

- EU AI Act 대응
  - 해외에서는 EU AI Act가 본격적인 기준점이 되면서, AI 제품/서비스가 유럽 시장에 진출하려면 “좋은 기술”만이 아니라 EU AI ACT 요구사항을 충족했다는 증빙(적합성 평가)이 필수로 요구되는 구조가 강화되고 있음.
  - 이 과정에서 제3자 시험 검증 인증을 통해 객관적 근거를 확보하려는 수요가 자연스럽게 증가하고 있음.
- Trust Mark(신뢰 마크) 확산
  - 유럽·글로벌 시장에서는 소비자 및 기업 고객이 AI를 선택할 때, 단순 기능보다 “믿을 수 있는가”를 우선적으로 묻는 경향이 뚜렷해지고 있음. 이런 환경에서 Trust Mark(신뢰 마크)는 제품/서비스가 일정 수준의 신뢰 요건을 충족했음을 직관적으로 보여주는 인증제도가 각국에서 제정되고 있음.
- 안전/재현성(Reproducibility) 검증 트랙 강화
  - 해외에서는 알고리즘이 반복 가능한 결과를 내는지 재현성과 오작동 시 위험을 통제할 수 있는지 안전성에 대하여 강화하고 있으며, AI 운영 과정에서 변경관리, 성능평가, 모니터링, 사고 대응체계를 함께 갖추었는지가 점점 더 중요하게 다루어지고 있음.
- 윤리·사회적 영향 고려
  - AI가 사회에 미치는 영향까지 고려해야 한다는 요구가 커지면서 윤리·사회적 영향 중심의 인증/평가 프레임도 함께 강화되고 있음. 공정성·차별 방지, 프라이버시·설명가능성·책임성 같은 요소는 단지 선언으로 끝나는 것이 아니라, 실제 평가 항목과 체크리스트로 만들어지고 있으며, 조직이 이를 운영할 수 있는지(역량, 교육, 프로세스)까지 함께 평가하고 있음. 결과적으로 기업은 제품인증만 준비하는 것이 아니라, 윤리/거버넌스 체계까지 묶어서 대응해야 하는 방향으로 전환 중.

## AI 제품/서비스 관련 법령 및 규정

- AI 기본법: 2024-12 통각(‘AI 컨트롤타워’·안전연구기관 근거 등), 2025-01 제정 확인·2026 시행 예정
- EU AI Act(Regulation (EU) 2024/1689): 세계 최초의 포괄적 AI 규정. 위험기반 접근(금지·고위험·제한적·최소 위험), GPAI(범용 AI) 의무, 제재(최대 글로벌 매출의 7%) 등을 규정.
- OECD AI 원칙: 2024 개정(GPAI 등 최신 이슈 반영). 가치기반 원칙과 정책 권고 제공. 회원국 및 파트너 다수 채택.
- NIST AI RMF 1.0: 전 산업 자율 가이드(신뢰성 특성, 위험 식별/완화 프레임).

21

## 관련표준

구분	표준명	주요내용
ISO/IEC 42001:2023	Artificial Intelligence Management System (AIMS)	조직이 AI를 책임 있고 안전하게 개발·운영하기 위한 경영시스템 요구사항 규정. AI 정책, 역할 책임, 리스크 영향평가, 문서화, 내부심사, 경영검토, 지속적 개선 포함
ISO/IEC 22989:2022	Artificial Intelligence — Concepts and terminology	AI 시스템, 모델, 자동화 수준 등 AI 관련 기본 개념과 용어 정의. 이해관계자 간 공통 기준 제공
ISO/IEC 23894:2023	Artificial intelligence — Risk management	ISO 31000 기반 AI 특화 위험관리 가이드. 데이터 모델 운영 사회적 영향 리스크 식별, 분석, 평가, 처리 방법 제시
ISO/IEC 5338:2023	Artificial intelligence — AI system life cycle processes	AI 시스템의 전 생애주기(기획, 개발, 검증, 배포, 운영, 유지보수, 폐기) 프로세스 정의
ISO/IEC 23053:2022	Framework for Artificial Intelligence (AI) Systems Using Machine Learning	마신러닝 기반 AI 시스템의 구조, 구성요소, 상호작용에 대한 프레임워크 제공
ISO/IEC 38507:2022	Governance implications of the use of artificial intelligence by organizations	조직 차원의 AI 거버넌스 원칙과 경영진 책임, 의사결정, 통제 구조 가이드
ISO/IEC 25023:2016	Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement of system and software product quality	기능성, 성능효율성, 사용성, 신뢰성, 보안성 등 소프트웨어 품질 특성 및 측정 지표 정의
ISO/IEC 25051:2014	Software engineering — SQuaRE — Requirements for quality of Ready to Use Software Product (RUSP)	사용자 관점에서 소프트웨어 품질 요구사항과 시험 기준 제시
ISO/IEC 25059:2023	Systems and software engineering — SQuaRE — Quality model for AI systems	AI 시스템 특성을 반영한 품질 모델 제시(전통적 SW 품질과 AI 특성 연결)
ISO/IEC 5259 (시리즈)	Data quality for analytics and machine learning	AI 학습 검증 데이터의 품질 특성, 관리 원칙, 평가 기준 정의

## 인증기관

- AI+ 인증은 한국표준협회(KSA)에서 인증을 획득할 수 있으며 인공지능 기술이 적용된 제품이나 서비스의 품질과 신뢰성을 객관적으로 증명하기 위해 도입된 세계 최초의 AI 품질 인증 제도.

No.	기관명	주소	홈페이지	전화번호
1	한국표준협회	서울 강남	www.ksa.or.kr	02-6240-4662

22

## 인증현황

- 국내 주요 기업들이 이 인증을 획득하여, 자사 AI 서비스의 안전성과 신뢰성을 홍보하고 있음.
- 25년 12월 기준 약 50개 社, 97개 인증서 발급.

## 인증대상 제품/서비스

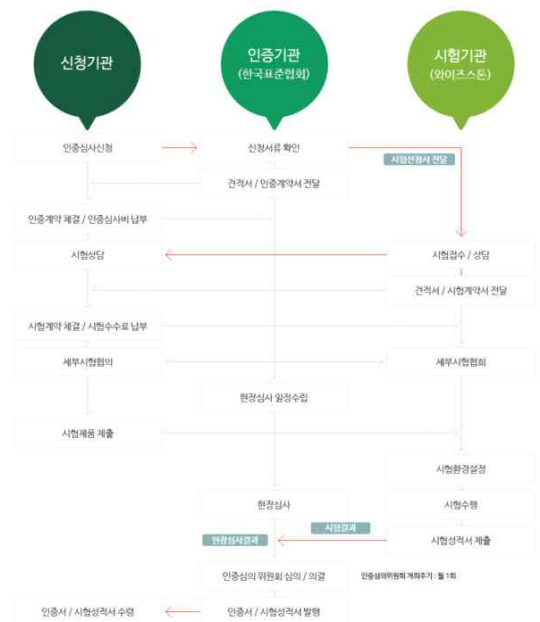
- AI+ 인증제도는 인공지능 기술이 적용된 소프트웨어(SW), 하드웨어(HW), 서비스 및 ICT 기반 제품 전반을 인증 대상으로 함.
- 즉, 단순히 ‘AI 기능을 내장한 제품’만이 아니라, AI를 핵심 구성요소로 활용하거나 AI 알고리즘을 통해 주요 의사결정, 분석, 제어, 예측, 추천 등의 기능을 수행하는 모든 시스템과 서비스가 인증 대상.
- AI+ 인증 대상 제품/서비스는 AI 제품, AI 서비스, AI 응용소프트웨어, AI 플랫폼 및 인프라, AI 융합 서비스로 다음과 같으며 이에 국한하지 않음.

대상	제품/서비스(예시)
AI 기반 제품	영상 음성 문자 인식 등 지능형 기능을 내장한 하드웨어 제품 예) CCTV 영상분석 장비, 자율주행 센서 모듈, 얼굴인식 출입통제기, 스마트가전, 로봇, 웨어러블 헬스기기 등
AI 기반 서비스	인공지능 모델을 활용하여 사용자에게 특정 판단, 추천, 분석, 모니터링, 예측 서비스를 제공하는 플랫폼 시스템 예) 챗봇 음성버서, AI 의료진단 서비스, 스마트팩토리 분석 시스템, 예지정비(PdM) 플랫폼, 교통/보안 모니터링 시스템, AI 기반 고객응대 서비스 등
AI 응용 소프트웨어	AI 모델 또는 마신러닝 알고리즘을 내장하거나 외부 AI 엔진과 연동되는 응용 프로그램 예) AI 에디터 플, 번역 서비스, 영상편집 자동화 도구, 문서요약 검색 엔진, 제조공정 최적화 SW 등
AI 플랫폼 및 인프라	AI 서비스를 개발·운영하기 위한 클라우드 플랫폼, 데이터 분석 환경, AI 운영관리시스템(MLOps, AIMS) 등 예) AI 학습/검증 데이터 관리 플랫폼, 모델 배포·모니터링 시스템, AI 운영 거버넌스 솔루션 등
AI 융합 서비스	산업·공공·사회 분야에서 AI가 다른 기술(IoT, Big Data, Cloud, 5G 등)과 융합되어 지능형 의사결정 또는 제어기능을 수행하는 복합 서비스 예) 스마트시티 교통관리, 재난안전 예측 시스템, 국방 감시정찰 AI, 지능형 에너지관리시스템(EMS), 헬스케어 모니터링 서비스 등

## 인증절차

- 인증절차는 ① 인증신청 → ② 신청서 검토 및 계약 → ③ 시험 상담 및 시험 계약 → ④ 세부시험 협의 → ⑤ 시험수행 → ⑥ 현장심사 수행 → ⑦ 인증심의위원회 심의 → ⑧ 인증서 및 시험성적서 발급 → ⑨ 인증완료 및 사후 관리

- 기업에서 AI+ 인증을 받는 절차를 기업 관점에서 쉽게 알 수 있도록 표현한 그림.



[그림 2-1] 인증 절차

## 인증신청

- AI+ 인증 신청서는 회사 정보, AI 제품/서비스의 실제 기능과 범위를 객관적이고 명확하게 설명하는 문서이며, 이후 시험 및 현장심사의 기준점.

- 조직 및 담당자 정보

- 기업명, 사업자등록번호, 대표자 성명, 본사주소
- 담당자 성명, 부서/직위, 연락처, 이메일 등

- 인증 신청 현황

- 인증신청 범위에는 제품명과 소프트웨어 버전을 작성.
- 활동은 설계/개발, 제조, 설치, 공사, 판매, 부가서비스, 기타 등에서 해당하는 부분에 체크.
- 인증 종류를 선택.

- 프리미어 : 인증조직의 품질경영시스템(설계/개발 프로세스를 포함하는 모든 비즈니스 프로세스)에 대한 현장심사를 실시하며, 신청 제품 및 서비스의 모든 기능(인공지능 기능을 포함하는 매뉴얼에 기재된 모든 기능)이 시험의 대상.
- 스탠다드 : 인증조직의 설계/개발 프로세스에 대한 현장심사를 실시하며, 신청 제품 및 서비스의 인공지능 기능(학습모델로 구현된 인공지능 모델이 적용된 기능)만이 시험의 대상.
- 신청한 제품 및 서비스의 개요 및 활용방법, 편익성(도입 전과 대비한 사용자에 대한 혜택 증가) 및 실제 사용자의 활용사례에 대하여 작성.
- 신청 제품 혹은 서비스에 적용된 학습모델(지도/비지도/강화) 및 특징을 작성.
- 학습 데이터, 입력 데이터 및 출력(결과값) 데이터에 대하여 작성.
- 인공지능 시스템 개발단계에서 검증(verification)한 성능지표 및 측정결과에 대하여 작성.
- 개발 방법론, 개발 프로세스(개발 규정 및 지침) 개요 및 개발과제 관리방법(요구사항정의서 관리, 개발진도 관리, 개발 산출물 관리)에 대하여 작성.

- 작성시 마케팅 문구가 아닌 사실 기반으로 설명을 작성하는 것이 좋으며, AI가 무엇을 어떻게 판단(분석)하는지 명확히 기재하는 것이 필요하며, 제품명/모델명/서비스명을 인증서에 반영되므로 정확히 작성 이 필요함. 불명확한 부분은 사전 상담 후 작성하는 것이 안전.

25

## 성능시험

- 성능시험은 ISO/IEC 25023, 25051 국제표준을 기반으로 품질특성 및 사용자 관점의 AI기능 시험을 진행, AI제품/서비스의 시험 항목과 시험 지표, 세부 지표는 다음과 같으며, 제품/서비스의 형태와 목적 에 따라 시험 항목과 적절한 지표를 설정할 수 있음.

심사항목	주요 심사 항목	심사 목적
AI모델성능	정확도 지표 (Accuracy)	정확도, 정밀도(Precision), 재현율(Recall), F1-Score 등 기본 성능 측정
	도메인 특화 지표	mAP(객체 인식), WER(음성 인식), BLEU(번역) 등 분야별 적합 지표
	임계치(Threshold) 설정	사용 목적에 부합하는 성능 목표치 수립 및 달성 여부 검증
AI 신뢰성	편향 및 공정성	데이터 및 결과의 편향성(Bias) 분석, 특정 그룹에 대한 차별 방지
	강건성 (Robustness)	노이즈, 데이터 변화 등 다양한 조건에서도 안정적으로 동작하는지 확인
	설명가능성 (XAI)	AI의 판단 근거를 사용자가 이해할 수 있는 형태로 제공하는지 평가
SW 품질	기능성 및 사용성	명시된 기능의 정확한 구현 및 사용자 인터페이스(UI/UX)의 편의성
	보안성 (Security)	데이터 보호, 접근 제어, 취약점 점검 등 SW 보안 요구사항 준수
	유지보수성	ISO/IEC 25051 등 품질 모델 기반의 수정, 업데이트 용이성 평가

## AI+ 인증 핵심 준비사항

- AI+ 인증은 AI 제품·서비스의 기획부터 폐기까지 전 과정에서 윤리성, 신뢰성, 안전성을 종합적으로 평가.
- 요구사항은 기획/설계, 데이터 획득/관리, 개발/AI 모델, 성능/품질관리, 제품/서비스 제공 및 운영, 서비스 운영(유지보수), 폐기 및 종료 등 전 생애주기 관리체계를 중점적으로 심사. 인증 요구사항은 책임 있는 AI 개발과 안전한 서비스 제공을 보장하기 위한 기준.

프로세스	핵심내용
기획/설계	기획단계에서 AI 제품·서비스의 목적 범위 설정, 이해관계자 요구 반영, 리스크 영향평가, 윤리 범위 검토 등이 적절히 이루어졌는지 평가
데이터 획득 / 관리	학습 검증 데이터의 출처, 품질, 편향, 윤리성, 법적 적정성 등을 관리하는 체계를 평가
개발 / AI 모델	AI 모델 설계·개발 단계에서 알고리즘 적합성, 오류 편향성 검증, 윤리 보안 고려 등이 이루어졌는지 평가
AI 성능 / 품질관리	AI 시스템이 정의된 성능지표(KPI)를 달성하고 있으며, 품질·안전·신뢰성 확보 및 모니터링 체계가 있는지 평가
제품/서비스 제공 및 운영	AI 제품/서비스가 사용자에게 제공되는 과정에서 안전하고 투명하게 운영되며 범위 인증 요구사항 이 준수되고 있는지 평가
서비스(유지보수)	AI 시스템의 유지보수 및 민원 사고 대응, 개선 활동이 체계적으로 이루어지고 있는지 평가
폐기 및 종료	데이터 삭제, 모델 종료, 기록 보존·폐기, 영향 종료에 대한 프로세스 및 기록이 체계적으로 이루어 지는지 평가

27

## 인증심사

- 기업에서 인공지능경영시스템 인증을 위해 준비해야 할 문서와 기록을 구분하여 요약.
- “경영문서”는 인공지능경영을 위한 계획과 프로세스 관련 문서.
- “운영기록”은 프로세스에 따라 실행한 결과를 입증하는 자료.

## 현장심사

- 현장심사는 AI 제품의 기획부터 폐기까지 책임성과 신뢰성을 확보하기 위하여 현장에서 문서 검토와 인터뷰 등을 통해 심사를 진행.
- AI 제품/서비스의 전 생애주기별 심사항목과 주요 평가 포인트, 목적을 정리한 요약표.

심사항목	주요 심사 항목	심사 목적
기획/설계	목적, 이해관계자, 리스크, 윤리 범위	AI 제품의 책임있는 기획 체계 확립
개발/모델	모델 적합성, 오류·편향 검증	기술적 신뢰성과 윤리성 확보
데이터 관리	품질, 법적·윤리 적정성, 이력관리	데이터 신뢰성과 공정성 보장
성능/품질관리	지표, 모니터링, 안전대책	AI 성능의 지속적 품질 보증
제공/운영	사용자 안내, 범위 준수, 계약 관리	책임 있는 서비스 제공 및 사용자 보호
유지보수	사고 대응, 개선, 종료관리	신뢰성 지속가능성 확보
폐기 및 종료	Data 및 모델, 알고리즘 폐기관리	데이터·모델·알고리즘 폐기 절차 준수
ISO/IEC 25051:2014	Software engineering — SQuaRE — Requirements for quality of Ready to Use Software Product (RUSP)	사용자 관점에서 소프트웨어 품질 요구사항과 시험 기준 제시
ISO/IEC 25059:2023	Systems and software engineering — SQuaRE — Quality model for AI systems	AI 시스템 특성을 반영한 품질 모델 제시(전통적 SW 품질과 AI 특성 연결)
ISO/IEC 5259 (시리즈)	Data quality for analytics and machine learning	AI 학습 검증 데이터의 품질 특성, 관리 원칙, 평가 기준 정의

26

적용표준 및 참고문서
<ul style="list-style-type: none"> <li>ISO/IEC 22989, ISO 31000, ISO/IEC 23894</li> <li>ISO/IEC 5259(데이터 품질), ISO/IEC 27701, ISO/IEC 27018</li> <li>ISO/IEC 23053, ISO/IEC 5338, ISO/IEC 23894</li> <li>ISO/IEC 23894, ISO/IEC 27001, TR 24368</li> <li>ISO/IEC 27035(Incident Management), ISO/IEC 38507</li> <li>ISO 9001, ISO 31000, ISO/IEC 19011</li> <li>ISO/IEC 27001, ISO/IEC 20889(비식별화)</li> </ul>

- 인증 현장심사 체크리스트는 단계별 심사 흐름, 주요 점검 활동, 핵심 요구사항으로 구성되며, ‘단계’는 기획부터 폐기까지의 절차를, ‘주요 활동’은 각 단계에서 수행해야 할 심사 포인트를 의미.
- ‘핵심요구사항’은 AI 시스템의 신뢰성·윤리성·안전성 확보를 위한 필수 기준을 제시함.

### 1. 기획 및 설계 단계

주요 활동	핵심 요구사항(문서)
<ul style="list-style-type: none"> <li>AI 시스템 목적 정의</li> <li>이해관계자 요구사항 식별</li> <li>리스크 및 영향 평가 기획</li> <li>윤리 범위 검토</li> </ul>	<ul style="list-style-type: none"> <li>조직의 AI 정책 수립 및 문서</li> <li>책임 및 역할(R&amp;R) 정의 및 내부 조직 구성</li> <li>AI 리스크 및 영향 식별 평가 처리 프로세스 및 관련 문서 AI 제품/서비스 기획 시 이 이해관계자(사용자, 사회 등) 요구사항 반영 및 문서</li> </ul>

### 2. 데이터 획득 및 준비 단계

주요 활동	핵심 요구사항(문서)
<ul style="list-style-type: none"> <li>데이터 수집 라벨링</li> <li>품질 및 편향 관리</li> <li>보안 프라이버시 검토</li> <li>데이터 출처 관리</li> </ul>	<ul style="list-style-type: none"> <li>데이터 품질·출처·이력관리 문서화 및 실행</li> <li>데이터 획득·사용에 대한 법률·윤리적 타당성 확보 및 문서</li> <li>학습 검증 데이터 전처리 라벨링 이상치 처리 변경이력 관리 프로세스</li> <li>제3자(협력사·데이터 공급자) 관계 관리 체계</li> </ul>

### 3. 개발/AI 모델 단계

주요 활동	핵심 요구사항(문서)
<ul style="list-style-type: none"> <li>알고리즘 선택 및 학습</li> <li>모델 검증·테스트 설계</li> <li>편향 및 과적합 검토</li> <li>기술문서화(SRS/FRS 포함)</li> </ul>	<ul style="list-style-type: none"> <li>AI 시스템 개발단계의 산출물</li> <li>모델 개발에 필요한 자원 식별 및 관리</li> <li>모델 검증·시험 프로세스 수립 및 실행에서의 오류, 편향, 안전성 검토</li> <li>윤리적 설계(공정성·투명성) 및 보안 프라이버시 설계 여부</li> </ul>

28

4. AI 성능/품질관리 단계

주요 활동	핵심 요구사항(문서)
<ul style="list-style-type: none"> <li>- 기능 성능 신뢰성 검증</li> <li>- 보안 및 윤리적 점검</li> <li>- 객관적 검증</li> </ul>	<p>성능 품질관리 실행 및 지속적 평가 프로세스</p> <p>AI 시스템 운영 중 오류 이상 탐지 및 대응체계 마련</p> <p>외주 협력사 개발 모델에 대한 품질관리 및 책임배분 체계</p> <p>제품 및 서비스의 기술 및 안전성 기준 반영 여부</p>

5. 제품/서비스 제공 및 운영 단계

주요 활동	핵심 요구사항(문서)
<ul style="list-style-type: none"> <li>- AI 시스템 배포 모니터링</li> <li>- 로그 기록</li> <li>- 이상탐지 및 보안관리</li> <li>- 사용자 피드백 반영</li> </ul>	<ul style="list-style-type: none"> <li>- 운영 범위 책임 소재 사용자 안내 문서화</li> <li>- 사용자 매뉴얼 제한사항 안내 피해구제 절차 마련</li> <li>- 운영환경에서의 법규준수 및 인증(예: 개인정보보호, 안전인증) 고려 인간감독 사회적 영향 책임성 기준 반영</li> </ul>

6. 서비스 (유지보수)

주요 활동	핵심 요구사항(문서)
<ul style="list-style-type: none"> <li>- 지속적 개선 (성능·윤리·안전)</li> <li>- 버전관리 및 변경통제</li> <li>- 피드백 기반 재학습</li> </ul>	<ul style="list-style-type: none"> <li>- 모니터링 및 준수평가</li> <li>- 민원 사고 대응 프로세스 수립 및 이력관리</li> <li>- 지속적 성능모니터링 및 피드백 마련</li> </ul>

7. 폐기 및 종료

주요 활동	핵심 요구사항(문서)
<ul style="list-style-type: none"> <li>- 데이터 삭제·보관정책 준수</li> <li>- 기록보존 및 재현성 확보</li> <li>- 자산 재활용·폐기 관리</li> </ul>	<ul style="list-style-type: none"> <li>- 데이터 및 모델 폐기 규정 준수 여부</li> <li>- 로그 기록 등 보존 여부</li> </ul>

인증 표시 사항

- 인공지능(AI, artificial intelligence)을 의미하는 'AI'와 우측 상단 품질 향상을 뜻하는 '플러스(+)'를 표현. 우측 상단 '플러스'는 무한대(Infinity)를 뜻하는 기호 '∞'를 겹쳐 형상화한 디자인으로, AI+ 인증이 세상 모든 인공지능 제품의 품질을 증명하는 글로벌 품질 인증으로써 무한하게 뻗어 나간다는 의미.
- 인증 마크는 인증받은 범위에 해당하는 제품, 제품포장 또는 홍보물(온라인 포함)에 사용할 수 있음.



[그림 2-2] AI+ 인증 마크

29

AI+ 로고 표시방법



인증 기간 및 비용 (KSA)

- 인증 비용

구분	신청비	현장심사비	시험수수료	인증마크사용료
대기업	50만원	300만원 (1개제품기준, 3MD) +50만원/추가제품당(0.5MD)	신청기관과의 협의를 통해 별도의 시험수수료 신청 기준에 따라 정함	1-3제품: 500만원 4-6제품: 1,000만원 7제품 이상: 1,500만원
중견기업		200만원 (1개제품기준, 2MD) + 50만원/추가제품당(0.5MD)		1-3제품: 300만원 4-6제품: 600만원 7제품 이상: 800만원
중소기업		200만원 (1개제품기준, 2MD) + 50만원/추가제품당(0.5MD)		1-3제품: 200만원 4-6제품: 400만원 7제품 이상: 600만원

※ 기업규모 구분 : 대기업(연 매출 1,000억 이상), 중견기업(500억 이상, 1000억 미만), 중소기업(500억 미만)

- 인증 비용 : AI+ 심사 비용은 제품당 산정되며, 중소·중견기업은 평균 800만~1,200만 원, 대기업은 평균 1,000만~1,500만 원의 비용이 소요됨.

- 제품 기준

- ICT 하드웨어 제품의 경우, 한국표준무역분류 항목표의 세부류 품목과 신청 제품의 복수 모델 현황을 기준으로 정함.
- 소프트웨어(어플리케이션, 솔루션 패키지 등) 제품의 경우, 사용자(소비자) 관점을 기준으로 별도 협의 하여 정함.
- 시험 기능/소요 일수 별 예상 시험 수수료
- 시험 대상, 시험 범위, 시험 횟수, 시험 장소 등 여러 조건에 따라 변경될 수 있으므로 별도 협의하여 정함.

30

FAQ

<p><b>1) AI+ 인증이란 무엇인가요?</b></p> <p>AI+ 인증은 인공지능 기술이 적용된 제품·서비스의 품질, 신뢰성, 안전성을 객관적으로 검증하는 인증제도입니다. AI 모델 성능시험과 함께 조직의 AI 운영 관리체계를 심사하여, 신뢰할 수 있는 AI임을 공식적으로 입증합니다.</p>
<p><b>2) AI+ 인증은 어떤 제품이나 서비스가 대상인가요?</b></p> <p>AI 기술이 적용된 모든 소프트웨어, 서비스, ICT 제품이 대상입니다. CCTV 영상분석, 출입통제, 챗봇, 생성형 AI, 금융·의료 AI, 스마트팩토리, AI 플랫폼 등 산업 분야 제한 없이 신청할 수 있습니다.</p>
<p><b>3) AI+ 인증은 제품 인증인가요, 시스템 인증인가요?</b></p> <p>AI+ 인증은 제품·서비스 인증이지만, 단순 성능시험을 넘어 ISO/IEC 42001 기반의 운영체계를 함께 평가하는 복합형 인증입니다.</p>
<p><b>4) ISO/IEC 42001 인증을 이미 받았으면 AI+ 인증이 필요 없나요?</b></p> <p>아닙니다. ISO/IEC 42001은 조직의 관리체계 인증, AI+는 개별 제품·서비스 인증이므로 상호 보완 관계입니다. 두 인증을 함께 보유 하면 규제 대응력과 대외 신뢰도가 더욱 강화됩니다.</p>
<p><b>5) AI+ 인증을 받으면 EU AI Act 대응에 도움이 되나요?</b></p> <p>네. AI+ 인증은 위험관리, 데이터 관리, 성능 검증, 운영 통제 등 EU AI Act의 핵심 요구사항과 정합성이 높아, 유럽 시장 진출 시 사전 준비 및 증빙 자료로 활용할 수 있습니다.</p>
<p><b>6) 인증 과정에서 어떤 평가가 이루어지나요?</b></p> <p>주요 평가는 다음 두 가지로 구성됩니다. 제품시험: AI 모델 성능, 신뢰성(편향·강건성·설명가능성), 소프트웨어 품질 현장심사: AI 기획·개발·운영 유지보수·폐기 전 과정의 관리체계</p>
<p><b>7) 인증 준비를 위해 반드시 갖춰야 할 문서는 무엇인가요?</b></p> <p>필수 문서는 아니지만, 아래 자료가 있으면 심사가 원활합니다.         <ul style="list-style-type: none"> <li>- 제품/서비스 설명서</li> <li>- AI 기능 및 아키텍처 설명 자료</li> <li>- 사용자 매뉴얼</li> <li>- AI 관련 내부 정책 절차</li> <li>- AI 개발에 따른 산출물 (데이터 포함)- 리스크 평가: 실패/오작동/보안사고/규제위반 등 발생 가능성과 피해 중심</li> <li>- 영향평가: 개인정보, 차별, 인권, 안전, 이해관계자 피해 등 사회·인권·사용자 영향 중심</li> <li>- 리스크와 영향평가를 한 시드로 운영해도 되지만, 판단 기준과 산출물(결과 기록)은 구분되는 게 좋습니다.</li> </ul> </p>

31

참고자료

- ISO/IEC 42001:2023 - Artificial intelligence - Management system 인공지능 경영시스템의 요구사항을 규정하며, 조직이 AI 정책, 목표, 리스크 및 윤리적 기준을 수립하고 관리할 수 있도록 하는 거버넌스 표준.
- ISO/IEC 5338:2023 - Artificial intelligence - AI system life cycle processes AI 시스템의 정의, 통제, 관리, 실행, 개선을 위한 전 생애주기(Lifecycle) 프로세스를 규정하며, 기획부터 종료·폐기까지의 절차를 제시.
- NIST AI Risk Management Framework (AI RMF 1.0, 2023): 미국 National Institute of Standards and Technology에서 발표한 AI 리스크 관리 프레임워크로, AI 설계·개발·운영 전 단계에서 신뢰성과 책임성을 확보하는 데 활용.
- OECD AI Principles (2024): AI 시스템의 수명주기를 포함해 혁신, 인권, 민주주의, 투명성, 안전성 등을 담은 고수준 국제 가이드라인.
- Nemko Digital AI Trust Mark (2023): 노르웨이 Nemko Group이 운영하는 AI 신뢰성 인증제도로, ISO/IEC 42001과 EU AI Act를 기반으로 윤리적, 투명성, 공정성, 보안성, 책임성을 평가하여 신뢰 인증(Trust Mark)을 부여.

32

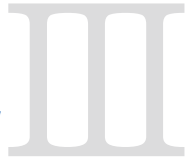


## Part. 03

### 실무 가이드 및 체크리스트



## 해외인증 실무 가이드북



## 부록

### 1. 인증 심사 프로세스 개요

34

### 인증 심사 프로세스 개요

문서 심사 (Stage 1 Audit)	<ul style="list-style-type: none"> <li>- AI 경영 매뉴얼 검토</li> <li>- AI 방침 및 목표 확인</li> <li>- 적응성 선언서 (SoA) 적절성</li> <li>- 리스크 평가 방법론 검증</li> </ul>
▼	
현장심사 (Stage 2 Audit)	<ul style="list-style-type: none"> <li>- 프로세스 이행 여부 확인</li> <li>- 담당자 인터뷰 수행</li> <li>- 운영 측정(로그/기록) 샘플링</li> <li>- 효과성 평가 검증</li> </ul>
▼	
부적합 대응 (NC Resolution)	<ul style="list-style-type: none"> <li>- Major NC : 인증 보류, 3개월 내 시정 및 재심사</li> <li>- Minor NC : 시정조치 계획서 제출 후 인증</li> <li>- 근본 원인 분석 (RCA)</li> </ul>
▼	
인증서 발급 (Issuance)	<ul style="list-style-type: none"> <li>- 심의위원회 최종 승인</li> <li>- 인증서 발행 (유효기간 3년)</li> <li>- 인증 마크 사용 권한 부여</li> <li>- 대외 홍보 및 마케팅 활용</li> </ul>
▼	
사후 심사 (Surveillance)	<ul style="list-style-type: none"> <li>- 연 1회 정기 심사 (1년차/2년차)</li> <li>- 주요 변경 사항 중점 확인</li> <li>- 지속적 개선 활동 점검</li> <li>- 3년차에 경신 심사 진행</li> </ul>

- Stage 1 심사에서 발견된 '우려 사항(Area of Concern)'은 Stage 2에서 중점적으로 다뤄짐.
- 문서 심사 후 즉각적인 보완 조치가 심사 통과율을 높이는 핵심 전략.

### SoA 작성 프로세스

리스크 평가 연동	- 식별된 AI 리스크 및 영향평가 결과를 바탕으로 필요한 통제 식별
▼	
통제 항목 선택	- 38개 항목 중 조직 상황에 맞는 통제 선택(또는 추가 통제 신설)
▼	
포함/제외 사유 기록	- 선택한 이유(법적 요구, 리스크 대응)와 제외한 정당한 사유 문서화
▼	
적용성 보고서 (SoA)	- 최종 문서 확정 및 경영진 승인 (심사 시 핵심 제출 자료)

34

### 문서 체계 및 템플릿

AI 경영 매뉴얼 (AI Management Manual)	<ul style="list-style-type: none"> <li>- 통합 매뉴얼</li> <li>- AIMS 적용 범위</li> </ul>	<ul style="list-style-type: none"> <li>- 조직 소개 및 구조</li> <li>- 프로세스 맵 (Process Map)</li> </ul>
방침 및 절차서 (Policies & Procedures)	<ul style="list-style-type: none"> <li>- AI 방침 (AI Policy)</li> <li>- AI개발 및 관리 절차</li> <li>- 비상대응 및 사고처리 대응 절차</li> </ul>	<ul style="list-style-type: none"> <li>- 리스크 및 영향평가 관리 절차</li> <li>- 변경 관리 절차</li> </ul>
작업 지침서 (Work Instructions)	<ul style="list-style-type: none"> <li>- 데이터 관리 지침</li> <li>- 모니터링 작업 지침</li> <li>- 도구(Tool) 사용 매뉴얼</li> </ul>	<ul style="list-style-type: none"> <li>- 모델 배포 지침</li> <li>- 심사 준비 지침</li> </ul>
양식 및 기록 (Forms & Records)	<ul style="list-style-type: none"> <li>- 데이터 카드 템플릿</li> <li>- 내부 심사 체크리스트</li> <li>- 경영 검토 회의록</li> </ul>	<ul style="list-style-type: none"> <li>- 모델 카드 템플릿</li> <li>- 리스크 및 영향평가 양식</li> </ul>

### 필수 증빙 자료 목록

AI 시스템 인벤토리	조직 내 모든 AI 시스템의 식별, 용도, 적용 범위 및 위험 등급 분류 기록
AI 방침 문서	AI 윤리 원칙 및 관리 목표가 포함되고 최고경영자가 승인한 공식 문서
리스크 평가 보고서	조직 관점의 재무/운영/법적 리스크 식별 및 평가 결과
AI 영향평가(AIIA)	개인 및 그룹, 사회에 미치는 영향 분석 보고서
적용성 보고서 (SoA)	통제 항목(Annex A)의 채택/제외 여부와 그 정당성 근거 문서
데이터/모델 카드	데이터셋 스킴, 모델 아키텍처, 성능 지표 등이 기술된 기술 명세서
변경 관리 로그	모델 업데이트, 데이터 재학습 등 주요 변경 사항에 대한 승인 기록
모니터링 대시보드	운영 중인 모델의 성능, 공정성, 드리프트(Drift) 상태 모니터링 기록
내부 심사 기록	자체 심사 결과 보고서, 부적합 사항(NC) 및 시정조치(CAPA) 완료 증거
경영 검토 회의록	AIMS 성과에 대한 최고경영진의 검토 및 자원 할당 등 의사결정 기록

### 표준간 주요 사항 비교

ISO 9001 (품질)	ISO/IEC 27001 (정보보호)	ISO 45001 (안전보건)	ISO/IEC 42001 (AI 경영)
품질 경영 범위 이해관계자 요구사항	ISMS 범위 (SoA) 정보 자산 식별	안전보건 범위 근로자 참여	AI 시스템 적용범위 AI 역할(제공/사용) 정의
품질 방침 고객 중심 경영	정보보호 방침 역할 및 책임	안전보건 방침 협의 및 참여	AI 방침 수립 (윤리,안전,투명성 원칙)
품질 리스크 / 기회 변경 계획	정보보호 리스크 평가 리스크 처리 계획	위험요인 파악 법적 요구사항	AI 리스크 평가 AI 시스템 영향평가 (AIIA)
인적 자원 역량 및 인식	인식 및 교육 보안 서약	의사소통 문서화된 정보	AI 역량강화 교육 데이터 카드 & 모델 카드
제품 실현 계획 설계 및 개발	운영 계획 및 통제 정보보호 처리	운영 통제 비상사태 대비	AI 수명주기 통제 (데이터-개발-검증-운영)
고객 만족 모니터링 및 측정	보안 효과성 측정 내부 심사	준수 평가 성과 모니터링	모델 성능 모니터링 (공정성,정확도,Drift)
부적합 등 시정조치 지속적 개선	정보보호 사고 관리 시정 조치	사고 조사 시정 조치	AI 비상상황 대응 모델 재학습 및 평가

### 흔한 실수 및 대응 방안

- ISO/IEC 42001 구현 및 심사과정에서의 주요 실패 요인 (Common Pitfalls)

실수 사례	대응 방안
1) AI 시스템 범위 과소/과대 정의	범위를 너무 좁혀 핵심 AI를 누락하거나, 너무 넓혀 통제 불가능한 영역까지 포함하는 오류. 논리적/물리적 경계를 명확히 해야 함.
2) 리스크와 영향 평가 혼동	조직의 재무적 리스크와 AI가 사회에 미치는 영향을 구분하지 않고 혼용하는 경우, 별도의 평가 기준(Criteria) 수립이 필수.
3) 데이터 출처 및 관리 미흡	학습 데이터의 출처와 가공 과정을 추적할 수 없어 신뢰성을 입증하지 못함. 데이터 버전 관리 도구 도입이 필요.
4) 제3자 벤더 통제 누락	외부 API나 솔루션 사용 시 책임 공유 모델을 정의하지 않아 보안 공백이 발생하며, 공급망 리스크 평가가 선행되어야 함.
5) 운영 모니터링 미흡	AI시스템의 사용에 따른 성능의 임계치 및 성능저하 주기에 대한 주기적 설정 미흡
6) 문서만 작성하고 실행 안함 (Paper Tiger)	심사만을 위해 문서를 급조하고 실제 운영은 다르게 하는 경우임. 심사원은 실제 운영 로그와 증거를 대조하여 이를 적발.
7) 경영진 관여 부족	AI 거버넌스를 실무자 선에서만 처리하고 경영진은 보고만 받는 경우입니다. 최고경영자의 리더십 증빙(회의록 등)은 필수 심사 항목.

● 주요 질문 사례

- 일반사항
- 심사원은 단순한 문서 확인을 넘어, 실제 담당자가 해당 절차를 이해하고 실행하고 있는지 '인터뷰'를 통해 심층 검증.

	주요 질문 사례
적용 범위	AI 시스템의 범위를 어떻게 정의했습니까? 물리적, 논리적 경계가 명확합니까?
영향 평가	고영향 시스템에 대한 AI 영향평가(AIIA)를 수행했습니까? 결과는 문서화되었습니까?
데이터 관리	데이터에 대한 출처와 관리 현황을 확인할 수 있습니까? 데이터 품질은 어떻게 보증합니까?
모니터링	모델 드리프트(Drift)를 어떻게 탐지하고 대응합니까? 재학습 임계값은 설정되어 있습니까?
제3자 관계	제3자 AI 공급업체(API 포함)를 어떻게 평가하고 관리합니까? 책임 소재는 명확합니까?
시정조치	AI 인시던트(침각, 편향 등) 발생 시 구체적인 대응 프로세스가 마련되어 있습니까?

● 핵심 심사 질문 TOP 10

- 세부사항
- 아래 질문에 대해 '증거(Evidence)'으로 답변할 수 있다면, 주요 부적합(Major Non-conformity) 리스크는 90% 이상 해소된 것.

	심사 준비 체크리스트 (Audit Readiness Checklist)
1	AI 시스템 인벤토리가 포괄적이며 최신 상태로 유지되고 있는가?
2	고영향 시스템에 대해 AI 영향평가(AIIA)가 수행되었는가?
3	데이터 출처, 품질 및 계보(Lineage)에 대한 거버넌스가 명확한가?
4	편향성 테스트 및 완화 전략이 문서화되어 적용되는가?
5	모델 드리프트(Drift) 탐지를 위한 지속적인 모니터링 체계가 있는가?
6	AI 의사결정에 대한 설명이나 근거를 제공할 수 있는가?
7	제3자 AI 공급업체를 계약 및 평가를 통해 관리하는가?
8	AI 실패 및 오류에 특화된 인시던트 대응 절차가 정의되었는가?
9	최고 경영진이 AI 성과와 규제 준수를 정기적으로 검토하는가?
10	AI 윤리 원칙이 조직 전체에 효과적으로 전파되었는가?

해외인증 실무 가이드북 (60. 인공지능)

발행일	2025년 12월 31일
발행처	산업통상부 해외인증지원단
주소	06160 서울시 강남구 테헤란로 69길 5(삼성동, DT센터 3층)
전화번호	02-6240-4770
이메일	globalcertification@ksa.or.kr
홈페이지	https://globalcerti.kr
감수	<b>KSA 한국표준협회</b>
작성	PwC컨설팅                      한국인정지원센터

© 수출유망품목 가이드북 (60. 인공지능)  
본 저작물은 산업통상자원부 해외인증지원단 소유이므로 사전 승인 없이 무단 전재와 복제를 금합니다.