

ISO/IEC 42001 : 2023

AI 거버넌스와 글로벌 규제 동향

1. AI 거버넌스란 무엇인가? – 윤리, 규제, 통합관리 관점에서

● AI 윤리

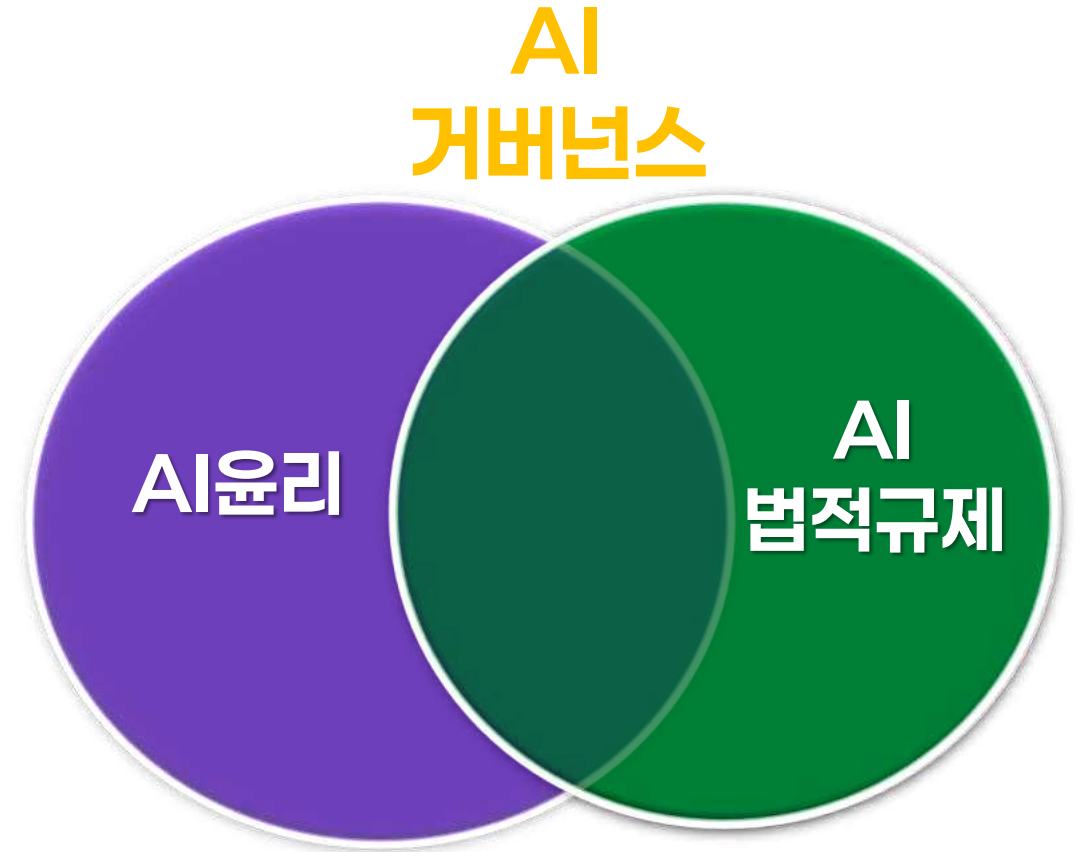
- ◀ 공정성·투명성·책임성 등 AI 개발과 활용의 판단을 이끄는 윤리 원칙
- ◀ OECD AI 원칙, UNESCO 권고안 등 참고

● AI 법적 규제

- ◀ AI 개발·제공·이용에 적용되는 법적 의무와 책임을 규정
- ◀ 적용 대상과 역할에 따라 준수해야 할 요구사항이 달라짐
예: EU AI Act, 한국 인공지능기본법 등

● AI 거버넌스

- ◀ 조직의 AI 의사결정·책임·감독을 연결하는 관리체계
- ◀ 윤리 원칙과 적용 법규를 정책·역할·절차에 반영
- ◀ ISO/IEC 42001 등 국제표준을 관리체계 구축에 활용
- ◀ 위험·영향 평가, 운영 점검, 이해관계자 소통과 개선 포함



윤리·법규를 조직의 의사결정과 운영에 반영

1.1 AI 위험관리 — 사용 목적과 영향을 함께 평가

● 위험 검토가 중요한 활용 사례

- 생체인식·감시 기능을 활용하는 AI
- 의료 진단·치료를 지원하는 AI
- 사법적 판단·채용 평가를 지원하는 AI
- 자율주행·드론의 안전 관련 AI



● AI 위험관리의 주요 확인 사항

- ① 사용 목적·이용 환경·영향받는 사람 파악
- ② 오류·편향·데이터·보안 등의 위험 식별
- ③ 발생 가능성과 영향 평가, 대응 조치 결정
- ④ 조치의 효과 확인, 운영 중 점검과 재평가



● 관련 법률·표준·프레임워크

- ISO/IEC 42001 — AI 경영시스템 표준
- NIST AI RMF — 자발적 위험관리 프레임워크
- EU AI Act — 용도·위험에 따른 법적 요구사항

위 사례가 모두 법적 고위험·고영향 AI에 해당하는 것은 아니며,
해당 법률의 적용 기준을 별도로 확인해야 합니다.

1.2 신뢰할 수 있는 AI — 원칙을 운영과 검증으로 연결

● 신뢰할 수 있는 AI의 주요 원칙

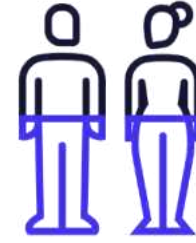
- **공정성** — 부당한 차별과 유해한 편향을 확인·완화
- **투명성** — AI의 용도·성능·한계와 필요한 설명을 제공
- **책임성** — 의사결정과 대응의 역할·책임을 명확화
- **안전성·보안성** — 사람에 대한 위해와 공격·오용 위험을 관리
- **프라이버시 보호** — 개인정보 처리 전반에서 권리와 정보를 보호

● 원칙을 실천하는 방법

- 사용 목적에 맞는 성능·신뢰성과 한계 검증
- 필요한 설명 수준에 맞춰 설명 방법·XAI 활용 검토
- 사람의 검토·개입과 문제 대응 절차 운영
- 운영 중 모니터링과 정기·변경 시 평가

● 조직에서 확인할 증거

- 성능·편향·안전성 등의 평가 결과와 개선 기록
- 이용자 안내와 개인정보 보호 조치
- 담당자의 검토·승인 및 문제 대응 기록



공정성
(Fairness)



투명성
(Transparency)



책임성
(Accountability)



안전성·보안성
(Safety & Security)



프라이버시 보호
(Privacy Protection)

2. EU AI Act, 제정에서 실제 적용의 단계로

2.1 2026년 8월 2일, EU AI Act의 다수 규정 적용과 집행 본격화 위험과 용도에 따라 달라지는 규제

EU AI Act는 위험과 용도에 따라 다르게 규율합니다

금지되는 AI 관행

조작, 취약성 악용, 일부 사회적 평가 등

고위험 AI

채용, 교육, 필수 서비스, 법집행 등 기본권과 기회에 중대한 영향을 미치는 일부 용도

투명성 의무 대상

챗봇 등 AI 상호작용, AI 생성·조작 콘텐츠, 딥페이크 등

범용 AI 모델

별도의 투명성·저작권 및 일부 모델의 시스템 위험 관련 의무

고위험 AI에 요구되는 관리 방향

- ◀ 위험평가와 완화
- ◀ 데이터 품질·거버넌스
- ◀ 기록과 문서화
- ◀ 사람의 감독(Human Oversight)
- ◀ 정확성·견고성·사이버보안



※ 주요 고위험 AI 의무: 일부 용도는 2027.12.2, 규제제품에 포함된 고위험 AI는 2028.8.2부터 적용

EU AI Act, 모든 AI를 똑같이 규제하지 않는다

01

금지되는 AI 관행 : 허용하기 어려운 특정 AI 활용 → 원칙적으로 금지



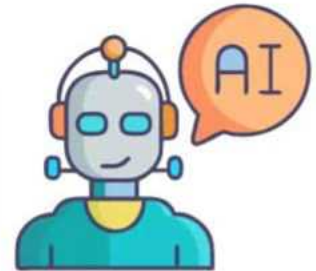
02

고위험 AI : 기본권·안전·기회에 중대한 영향을 미치는 일부 용도
→ 강화된 관리 의무



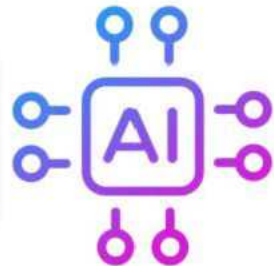
03

투명성 의무 : AI 상호작용·생성 또는 조작 콘텐츠 등
→ 이용자가 AI 사용 여부를 알 수 있도록 고지·표시



04

범용 AI 모델 : 여러 용도로 활용되는 기반 모델 → 투명성·저작권 등 별도 의무
→ 일부 모델은 시스템 위험 관련 추가 의무



2.2 미국과 한국, 서로 다른 방식으로 AI를 관리하다

미국: 혁신 촉진 + 분야별 위험관리

- AI 혁신과 산업 경쟁력 강화
- 연방 차원의 AI 정책 프레임워크 추진
- NIST AI RMF를 통한 자발적 위험관리
- 국가안보·사이버보안·조달 등 분야별 관리 강화

EU: 위험 기반의 포괄적 법률 규제

한국: 기본법 시행 + 조직 이행

- AI 기본법 2026년 1월 22일 시행
- 생성형 AI 등의 투명성 의무
- 고영향 AI의 위험관리
- 사람의 관리감독
- 시행령·가이드라인을 통한 이행 구체화



미국·EU·한국 규제 접근 한눈에 보기

미국

- ◆ 혁신 촉진
- ◆ 분야별 위험관리

EU

- ◆ 위험·용도 기반 규율
- ◆ 포괄적 법률 체계

한국

- ◆ AI 기본법 시행
- ◆ 신뢰 기반·조직 이행

같은 AI를 바라보지만, 규제와 관리의 방식은 다릅니다

글로벌 AI 활용에서는 기술뿐 아니라 적용되는 법과 관리체계를 함께 살펴야 합니다

기업들은 AI 신뢰성을 어떻게 관리하고 있을까?

기업	신뢰성 확보를 위한 접근	주요 운영 방식
Google	책임 있는 AI 거버넌스와 안전성 평가	AI 원칙, 다층적 테스트, Frontier Safety Framework
Microsoft	조직 전반의 Responsible AI 관리체계	Responsible AI Standard, 사전 검토, 투명성 보고
OpenAI	모델 출시 전 위험평가와 안전장치 검증	Preparedness Framework, System Card, 레드팀·안전성 평가

기업마다 방식은 다르지만, AI의 위험을 평가하고 책임을 정하며 운영 결과를 지속적으로 점검한다는 공통점이 있습니다.

이러한 활동은 ISO/IEC 42001의 위험관리·책임·모니터링 관점에서도 살펴볼 수 있습니다.

AI를 관리하는 서로 다른 도구: 법률 표준 프레임워크

구분	ISO/IEC 42001	EU AI Act	NIST AI RMF
성격	국제 경영시스템 표준	EU 법률	자발적 위험관리 프레임워크
중심 질문	조직은 AI를 어떻게 지속적으로 관리할 것인가	어떤 AI에 어떤 법적 의무가 적용되는가	AI 위험을 어떻게 식별·측정·관리할 것인가
주요 초점	책임·위험관리·운영·평가·지속적 개선	금지 관행·고위험 AI·투명성·범용 AI 등	거버넌스·맵락 파악·측정·관리 / (Govern · Map · Measure · Manage)
적용 방식	조직의 AIMS 구축·운영	적용 대상에게 법적 의무	조직이 필요에 맞게 자발적으로 활용
법률과의 관계	법규 준수를 지원하는 관리체계	법적 의무 그 자체	법률이 아닌 위험관리 지원 도구

“법률은 무엇을 준수해야 하는지를 정하고, ISO/IEC 42001은 조직이 AI를 관리하는 체계를 구축하도록 돕고, NIST AI RMF는 AI 위험을 식별하고 관리하는 데 활용할 수 있는 프레임워크를 제공합니다.”

서로 역할은 다르지만 실제 조직에서는 함께 활용될 수 있습니다

3. AI 거버넌스의 기본 틀, ISO/IEC 42001은 무엇을 요구하는가?

3.1 ISO/IEC 42001: AI 경영시스템(AIMS) 개요

- AI를 개발·제공·이용하는 조직을 위한 국제표준
- AI 경영시스템의 수립·실행·유지·지속적 개선 요구사항 제시

3.2 AI 경영시스템의 핵심 관리 흐름

- 조직 상황과 이해관계자 요구 파악, 정책·목표·책임 설정
- AI 위험·영향 평가와 대응 조치의 운영
- 성과평가·내부심사·경영검토를 통한 지속적 개선



ISO/IEC 42001:2023

※ ISO/IEC 42001은 2023년 12월 발행된 세계 최초의 AI 경영시스템 국제표준입니다.

윤리, 개인정보, 리스크 평가 등 AI 관리 전반을 포괄하며, 글로벌 AI 규제에 대응할 수 있는 관리 시스템의 기반을 제공합니다.

“ISO/IEC 42001은 단순한 기술 기준이 아닌, 글로벌 AI 신뢰성 확보의 출발점입니다.”



ISO/IEC 42001을 조직 운영에 적용할 때 살펴볼 실무 영역

1 AI 모델 관리 (Manage AI Models)

모델의 성능·한계 검증과 변경 시 영향 확인

✓ 실무 적용 예: 모델 성능 및 한계 평가

2 데이터 거버넌스 & 보안 (Data Governance & Security)

AI 데이터 품질 및 개인정보 보호

✓ 실무 적용 예: 안전한 데이터 관리 기준 적용

3 AI 알고리즘 편향 완화 (Algorithmic Bias Mitigation)

AI 의사결정의 공정성과 윤리성 확보

✓ 실무 적용 예: 편향 및 공정성 점검

4 AI 관리 체계 구축 (Establish AI Governance)

AI 운영을 위한 내부 프로세스 설계

✓ 실무 적용 예: 역할·책임과 관리절차 수립

💡 ISO/IEC 42001은 조직의 AI 경영시스템을 수립·운영하고 지속적으로 개선하기 위한 요구사항을 제공합니다.



ISO/IEC 42001을 조직 운영에 적용할 때 살펴볼 실무 영역

5 설명 가능성과 투명성 (Explainability & Transparency)

AI의 용도·성능·한계와 이용자에게 필요한 설명 제공

✓ 실무 적용 예: 이용자 안내, 결과 설명과 XAI 활용 필요성 검토

6 이해관계자 참여 (Engage Stakeholders)

관련 이해관계자의 요구를 파악하고 소통 방법 설정

✓ 실무 적용 예: 이용자 의견·불만 접수와 검토·대응 절차 운영

7 지속적인 모니터링 (Continuous Monitoring)

AI 운영 결과와 위험 변화 확인, 필요한 개선 조치 실행

✓ 실무 적용 예: 성과지표 점검, 계획된 주기의 내부심사와 후속 조치

💡 ISO/IEC 42001은 조직의 AI 경영시스템을 수립·운영하고 지속적으로 개선하기 위한 요구사항을 제공합니다.

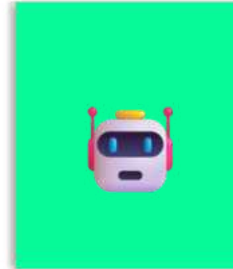
7

AI 거버넌스의 7가지 실무 영역 (ISO/IEC 42001 적용 관점)

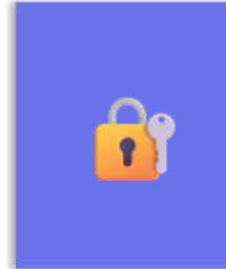
1. Manage AI Models
2. Data Governance & Security
3. Algorithmic Bias Mitigation
4. Establish AI Governance
5. Explainability & Transparency
6. Stakeholder Communication
7. Monitoring & Improvement

◆ 이 7개 영역은 학습을 위해 재구성한 실무 분류이며,
ISO/IEC 42001의 공식 조항 구분은 아닙니다.

01
AI 모델 관리



02
데이터 거버넌스
& 보안



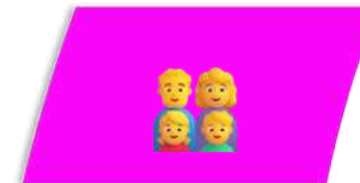
03
AI 알고리즘
편향 완화



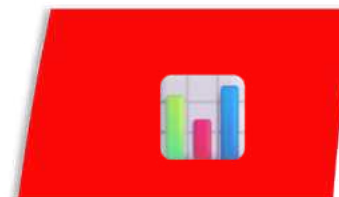
04 AI 관리체계 구축



05 설명 가능성과
투명성



06 이해관계자 소통



07 운영 모니터링과
개선





AI 거버넌스의 중심에는 사람의 판단과 책임이 있습니다

본 자료는 국제AI교육원의

ISO/IEC 42001 인공지능경영시스템 심사원보 양성과정 중

「AI 거버넌스와 글로벌 규제 동향」 강의 자료를

학습과 실무 이해를 위해 무료로 공개한 자료입니다.

휴먼 오버사이트 — 사람의 검토·판단·개입

AI의 결과를 확인하는 데서 그치지 않고,

사용 목적과 한계, 영향을 검토하며

필요할 때 수정하거나 사용을 중단할 수 있어야 합니다.

조직은 이러한 판단을 수행할 사람의 역할과 권한을 정하고,

검토와 조치의 기록을 남겨야 합니다.

AI 거버넌스를 관리체계와 심사 실무로 연결하고 싶다면

ISO/IEC 42001 심사원보 양성과정 자세히 보기 → <https://interaiedu.com/product/iso-iec-42001/>

자료 작성·제공: 국제AI교육원

작성일: 2026년 9월 21일

본 자료는 학습·참고용이며, 법률·정책의 실제 적용 시 최신 공식 자료와 조직에 적용되는 요구사항을 확인하시기 바랍니다.