

AX 전략 수립

AI 규제 원년, ISO 42001 기반 인공지능 경영시스템(AIMS) 구축

글 | Ackerton Partners, IE본부 이필화 상무



01 ·
현실로 다가온 AI 리스크,
우리의 현주소는?

02 ·
파편화된 대응의 한계

03 ·
파편화된 규제의 해법:
ISO/IEC 42001 기반
단일 통제 프레임워크

04 ·
사내 거버넌스 내제화
(3 Lines of Defense와
기술적 통제)

05 ·
맺음말

AI 리스크의 현실화와 규제의 동시다발적 발효

- 기밀 유출·편향성 등 치명적 AI 사고가 급증하고 2026년 글로벌 '복합 규제'가 발효됨에 따라, 과징금 방어를 위한 기업의 법적 '소명 책임' 이행이 필수 과제가 되었습니다.

파편화된 대응의 한계

- 부서별 사일로(Silo)식 중복 통제와 '새도우 AI' 남용을 막고 AX의 본질인 '의사결정 단축'을 달성하려면 전사 차원의 단일 통제 체계가 필요합니다.

파편화된 규제의 해법: ISO/IEC 42001 기반 단일 통제 프레임워크

- 기존 ISO/IEC 27001 체계를 뼈대로 'ISO/IEC 42001(AIMS)'을 구축하여, 일원화된 '통합 증적 자료'로 복합 규제를 일괄 방어해야 합니다.

사내 거버넌스 내재화 (3 Lines of Defense와 기술적 통제)

- 현업(1차)-컴플라이언스·보안(2차)-내부감사(3차)로 이어지는 '3차 방어선'을 확립하고, IAM·AI 전용 DLP·제로트러스트 등 기술적 통제를 결합해야 합니다.

맺음말

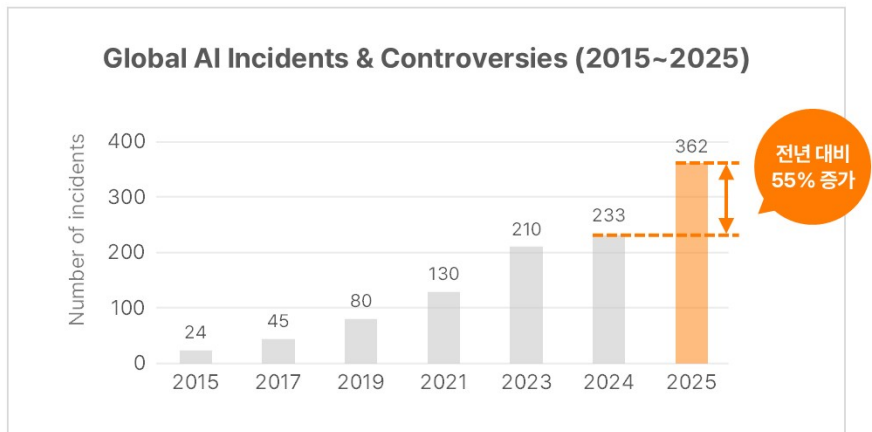
- 완벽한 브레이크가 과감한 가속을 돕듯, AIMS와 제로트러스트 인프라는 '신뢰할 수 있는 AI(Trustworthy AI)'를 증명하는 핵심 경쟁력이 될 것입니다.

01 현실로 다가온 AI 리스크, 우리의 현주소는?

1.1 수면 위로 떠오른 AI 리스크와 책임의 현실화

초창기 생성형 AI(Gen AI) 및 AI 에이전트 도입 시에는 단순한 '환각(Hallucination)' 현상이나 산출물의 품질 저하 정도가 문제였지만, 이제는 비즈니스 양상이 완전히 달라졌다. 오늘날의 AI 리스크는 기업의 핵심 영업 비밀 유출, 알고리즘 편향성, 나아가 자율형 에이전트의 오작동에 따른 물리적 피해까지 유발하며 비즈니스 연속성을 직접 위협하는 치명적 요인으로 진화했다. 특히 오픈소스 LLM 도입 시 라이선스 위반이나 악의적인 데이터 오염(Data Poisoning) 공격을 받는 등 기업이 독자적으로 방어하기 까다로운 외부 위협이 기하급수적으로 증가하고 있다.

[그림 1] 최근 10년간 글로벌 AI 관련 사고 및 논란 발생 추이



※ 출처 : Stanford University HAI(Human-Centered Artificial Intelligence), 'AI Index Report 2026' 데이터 기반 재구성

[표 1] 최근 3년 내 글로벌 주요 AI 사고 및 법적 분쟁 사례(2023~2025)

리스크 유형	발생 연도	발생 회사	사고 경위	결과	시사점
영업비밀 유출	2023년	국내 S전자	외부 생성형 AI(ChatGPT)에 사내 핵심 소스코드·회의록 무단 입력	• 사내 기밀의 외부 AI 서버 전송 및 학습 데이터 노출 • 사내 외부 생성형 AI 접속 차단	• 비인가 새도우 AI (Shadow AI) 통제 • AI 보안 가이드라인 필수
물리적 피해	2023~2024년	GM Cruise	자율주행 AI의 사고 직후 보행자 인식 오류 및 차량 오작동	• 보행자 중상 피해 및 벌금 부과 • 면허 박탈 및 로보택시 사업 전면 철수	• AI의 물리적 오작동이 기업의 비즈니스 연속성 을 직접 위협
챗봇/에이전트 오류 및 법적 책임	2024년	Air Canada	고객상담 AI 챗봇의 환각(Hallucination) 현상으로 허위 할인 규정 안내	• 기업의 AI 관리·감독 과실 인정 • 캐나다 재판소의 손해배상 판결	• AI 산출물 오류 및 오작동의 법적 귀책사유 는 도입 기업에 귀속
데이터·모델 오염	2024년	Byte Dance	내부 연구원의 상용 AI 학습 모델 코드·데이터 고의 조작(Sabotage)	• AI 모델 학습 프로젝트 방해 및 지연 • 약 110만 달러 손해배상 청구 소송 제기	• AI 학습 파이프라인 접근 통제 • 데이터 무결성 검증 필수
알고리즘 편향성	2024~2025년	Workday	AI 채용 이력서 평가 모델의 고령자·특정 인종·장애인 자동 탈락	• AI 공급사의 법적 차별 책임 인정 • 미 연방법원 대규모 집단소송 승인 (진행중)	• 인사/채용 AI의 데이터 편향 제재

1.2 AI 규제 본격 시행과 복합 규제 대응의 중요성

2026년은 한국 AI 기본법 전면 시행(1월)과 EU AI Act 전면 시행(8월)으로 명실상부한 'AI 규제 원년'이다. 여기서 경영진과 현업 실무진이 가장 간과하기 쉬운 함정이 바로 '복합 규제(Intersection of Regulations)'다. 사내에 단 하나의 AI 시스템을 도입하더라도 여러 법규의 통제망이 동시에 작동하기 때문이다.

[그림 2] 주요 국가의 AI 규제 현황

 AI 산업 발전과 규제의 균형 추구	 위험 수준에 따른 엄격한 규제	 AI 혁신 촉진과 위험 최소화 추구	 생성형 AI 중심의 강한 국가 통제
• AI 기본법 • 2026년 1월 22일 최초 시행 • 법률 • 고영향 AI 중심 • 최대 3,000만원 이하	• EU AI Act • 2026년 8월 2일 전면 시행 • 법률 • 고위험 AI 중심 • 최대 €35M (약 550억 원) 또는 전세계 매출 7% 이하	• NIST¹⁾ AI RMF²⁾ • 2023년 1월 26일 공개 • 가이드라인 (연방법 부재로 인한 주 정부/기관별 대응 강화 추세) • AI 위험 관리 및 신뢰성 확보 중심 • 과태료 없음	• AI 표시법 • 2023년 8월 15일 시행 • 행정규정 • 생성형 AI 중심 • 단일 과태로는 없으나 상위 법률로 처벌 연결 가능

1) NIST(National Institute of Standards and Technology)

2) AI RMF(AI Risk Management Framework)

예를 들어 EU AI Act의 경우, 고위험 AI 규정을 위반할 시 전 세계 연간 매출의 최대 7% 또는 3,500만 유로(약 550억 원)라는 천문학적인 과징금이 부과될 수 있다. 이에 따라 AI를 도입·운영하는 현업 부서는 기획한 서비스가 관련 법규의 통제 요건을 모두 적법하게 준수했음을 문서로 입증해야 하는 법적 '소명 책임'을 안게 된다.

02 파편화된 대응의 한계

복합 규제 환경에서 HR, IT, 법무, 정보보안 부서가 사일로(Silo)식으로 각기 다른 체크리스트로 통제를 적용하면, 통제 항목이 중복되거나 해석이 충돌하면서 혁신의 골든타임을 지연시킨다. 더불어 기업들은 흔히 AX(AI Transformation)를 '개인 업무의 단순 효율화'나 '편의성 증대' 정도로 오인하곤 한다. 이로 인해 구성원들은 전사적인 보안이나 규제 준수를 뒷전으로 미룬 채, 당장의 업무 처리 속도를 높이기 위해 통제 받지 않는 외부의 쉽고 빠른 비인가 AI 서비스(Shadow AI)를 무분별하게 사용하는 부작용이 발생한다. AX의 진정한 본질은 부서를 관통하는 '의사결정의 단축'에 있다. 파편화된 대응을 멈추고, 전사 관점의 단일 통제 체계와 명확한 거버넌스 원칙을 세워야 하는 이유가 바로 여기에 있다.

[그림 3] 단일 AI 시스템에 대한 다층적·복합 규제 교차 적용 예시

단일 AI 시스템에 대한 다층적·복합 규제의 교차 적용 예시

Use Case: 사내 AI 기반 인재 채용/평가 시스템



*적용 범위·의무 수준은 AI의 구체적 기능, 의사결정 영향도, 처리 데이터 및 적용 지역에 따라 달라질 수 있음

03 파편화된 규제의 해법: ISO/IEC 42001 기반 단일 통제 프레임워크

이러한 한계를 극복하기 위해서는 글로벌 공통 요구사항을 단일 프레임워크로 통합한 '인공지능 경영시스템(ISO/IEC 42001, AIMS)' 구축이 시급하다.

이 표준은 단순한 일회성 인증에 그치지 않고, PDCA(계획-실행-점검-개선) 사이클을 통해 사전 위험 평가부터 상시 모니터링에 이르는 전 과정을 체계화한다([그림 4] 참조). 특히 완전히 새로운 조직이나 체계를 신설할 필요 없이, 기존 ISO/IEC 27001(정보보호 경영시스템) 프로세스를 빠르게 활용하는 것이 가장 실효성 높은 전략이다([그림 5], [표 2] 참조). 이를 통해 기업은 다수의 글로벌 복합 규제가 요구하는 '소명 책임'을 일원화된 '통합 증적 자료'로 한 번에 방어할 수 있다.

더 많은 내용을 보시려면

파일 다운받기

버튼을 눌러주세요