# Responsible AI, 경영의 기본값

EY한영

Shape the future
with confidence

# AI 리스크, 이사회 안건으로 이동

이사회·C-Level의 책임 확대 → Top-Down 거버넌스와 실무 연계

**글로벌 동향**

AI Risk → 이사회 보고 대상 항목 편입
경영진 핵심 평가 기준 → 선제적 감독 여부

C-Level과 이사회의 적극적인 관리
↓
실무 부서의 통제 활동 효과적 작동

**EU AI Act, 각국 가이드라인**

| | |
|---|---|
| 이사회 | AI Risk 현황과 개선 계획을 공식 보고받아야함 |
| 위원회 | 독립적 점검 및 외부 검증 활용 감독 필요 |
| **C-Level** | AI 도입 시 영향·Risk가 통합 반영된 투자심의·Risk 심사 프로세스 구축 필요 |

✓ 경영진의 **AI Risk 허용 수준 (Risk Appetite)** 기반 모델·보안 등 세부 통제 절차를 설계·운영

! **'IT 부서만의 Risk'**로 남겨둘 경우, 이슈 발생 시 **경영진 차원의 대응 타이밍을 상실**

EY

# AI는 하나지만,
# 적용되는 규제는 여러 개

| | AI 기본법 | PIPA (개인정보 보호법) | 중대재해 처벌법 | 산업안전 보건법 | 제조물 책임법 | 노동·차별법 | 섹터 규제 |
|---|---|---|---|---|---|---|---|
| AI 채용·평가 | H | H | L | M | L | H | M |
| AI 대출·신용평가 | H | H | L | L | L | M | H |
| 스마트팩토리 AI | M | L | H | H | H | L | M |
| 자율주행 AI | H | M | H | M | H | L | H |
| 의료진단 AI | H | H | L | L | H | L | H |
| 생성형 AI 고객지원 | M | H | L | L | L | L | L |

H High
직접 적용, 주요 의무

M Medium
조건부 적용, 간접

L Low
일반적 적용, 통상 관리

EY

# Responsible AI의 실행 프레임

## NIST AI Risk Management Framework

| GOVERN | MAP | MEASURE | MANAGE |
|---|---|---|---|
| ▪ AI 위험 관리 문화·정책·책임 구조 수립<br>▪ 조직 전반의 AI 위험 허용 수준 정의 | ▪ AI 위험 식별·분류·맥락 파악<br>▪ 비즈니스 임팩트 및 이해관계자 분석 | ▪ AI 위험 분석·평가·우선순위화<br>▪ 정량적 위험 지표 측정 및 벤치마크 | ▪ AI 위험 대응·모니터링·지속 개선<br>▪ 위험 처리 계획 실행 및 효과 검증 |

## ISO/IEC 42001 – AI 경영시스템 국제표준(내부감사 관련 조항)

| 6.1 위험·기회 파악 | 8.1 운영 계획·통제 | 9.2 내부감사 | 10.1 지속 개선 |
|---|---|---|---|
| AI 위험 식별 및 기회 목록 체계화 | AI Lifecycle 전반 운영 통제 프로세스 | AI 경영시스템 내부감사 실시 의무 | AI 성과 기반 지속적 개선 문화 |

# Responsible AI 체크리스트

- [ ] AI 정책·윤리강령 수립 및 이사회 승인 완료
- [ ] AI 시스템 인벤토리 전사 관리 현황 확인
- [ ] 고위험 AI 식별 및 AI 영향평가(AIA) 실시
- [ ] 데이터 품질·편향 검증 프로세스 존재 여부
- [ ] AI 모델 설명가능성 확보 및 문서화
- [ ] AI 편향 테스트 정기 수행(최소 연 1회)
- [ ] AI 모델 성능 모니터링 체계 구축 여부
- [ ] AI 사고·이슈 보고 및 에스컬레이션 체계
- [ ] 내부감사의 AI 감사 계획 명시적 포함 여부
- [ ] 제3자 AI 벤더 관리·계약 조항 적절성

# Responsible AI의 의미

전체 내용은 EY.com에서 확인하세요.