SHIN&KIM
법무법인(유) 세종

법무법인(유) 세종

지속 가능한 AI 거버넌스 구현: 기업이 고려해야 할 3가지 체크리스트

2024.04. | 장준영 변호사 / AI센터 센터장

SHIN&KIM
법무법인(유) 세종

목 차

SHIN&KIM
법무법인(유) 세종

1. AI 리스크란

AI 리스크란

AI 기술 부작용, 사이버보안 불안은 향후 10년 내 전세계가 당면할 가장 큰 위험 중 하나 (WEF, 2024, Global Risk Report 2024)

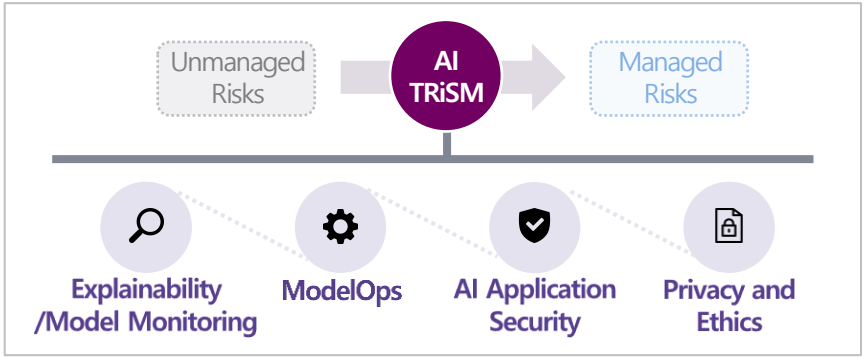
- 2023년 기업 경영에 위협을 가할 수 있는 위험 요소로 생성형 AI 가용성(mass generative AI Availability)이 새롭게 등장
- Gartner는 2024년 10대 전략 기술 트렌드 중 투자 보호 차원에서 선제적 AI 신뢰, 위험 및 보안관리(AI TRiSM, Artificial Intelligence Trust, Risk, and Security Management)를 제시
  - ❖ 전세계 AI TRiSM시장은 연평균 162%씩 성장, 2032년 74억 달러 규모를 형성할 것으로 전망(AMR, 2023)

[기업 경영에 위협을 가할 수 있는 위험 요소]

01	제3자 생존 위험 (Third-Party Viability Risk)
02	대량 생성형 AI 가용성 (Mass Generative AI Availability)
03	재정 계획의 불확실성 (Financial Planning Uncertainty)
04	클라우드 집중 위험 (Cloud Concentration Risk)
05	중국 무역 긴장(China Trade Tensions)

출처:Gartner (2023.8)

[AI 신뢰, 위험 및 보안관리 (AI TRiSM)]



출처:Gartner (2023). 4 Pillars of AI Trust, Risk, Security, Management to Manage Risk.

AI 리스크란

AI 리스크는 AI가 개인과 기업에 미칠 잠재적인 부정적 결과로서, AI 발전에 따라 더욱 다양한 형태로 진화할 것으로 예상

AI 기술에 내재된 리스크

공격 접점이 증가하는 위험 체인화(Risk Chaining)로, AI 모델 개발 시 예측하지 못한 사회적 리스크 우려

- 환각(hallucination), 데이터 편향, 오정보에 의한 왜곡, 오류, 설명책임의 한계 등 AI 기술이 가진 불안정성에서 오는 사회적 문제가 존재

데이터 활용에 따른 리스크

AI의 급속한 성장이 데이터의 외연적 확장에 기인한다는 점에서 AI는 데이터 활용에 따른 위험 요소를 내포

- 데이터에 의존하는 AI 활용이 수반하는 데이터 관련 리스크는 개인정보 오·남용, 유출·침해 사고 등 기업 보안 리스크에 직접적 영향을 미침

내부 통제가 불가한 리스크

AI 윤리·신뢰성 제고, AI 리스크 통제 위한 국내외 입법 시도로, 법 위반 리스크는 더욱 커질 것으로 전망

- 국제표준 미준수, 국내외 관련 법령 위반에 따른 제재 등은 결국 기업 비즈니스 리스크(경영/재무, 평판, 글로벌 진출 등)으로 이어짐

SHIN&KIM
법무법인(유) 세종

2. AI 리스크 관리 중요성

AI 리스크 관리 필요성

데이터 유출, 변조, 해킹 등 데이터를 기반으로 한 AI 잠재적 위험은 AI 생성, 도입 및 활용 전 과정에 항상 존재

- AI 리스크는 (i)기업이 기존에 경험하지 않아 익숙하지 않은 새로운 리스크(모델, 규정 준수, 운영, 글로벌 진출, 법률, 평판 및 규제, 리스크 등)로, (ii) 비즈니스 전반에 적용되어 기업 전체에 분산되어 위험 요인을 선별하기 어렵다는 특성을 가짐
  ❖ AI 리스크는 전통적 리스크와 비교 시, 상대적으로 리스크 정의의 명확성, 분류의 명확성, 데이터 가용성 등에서 한계가 존재

AI 활용에 따른 근원적 리스크 요인을 사전에 제거하지 않을 시, 기업은 회복할 수 없는 수준의 피해를 입을 가능성 증가

- 데이터 및 개인정보 보호, 사이버 보안 등 AI 기술 차원의 리스크를 관리하지 못할 경우 비즈니스 차원의 기업 피해(비즈니스 운영에 대한 피해, 보안 침해로 인한 피해, 조직 평판에 대한 피해 등)는 더욱 심각
- 매출, 수익에 상당한 영향을 미치는 기업의 통제 범위 밖에 있는 리스크를 사전에 어떻게 관리하는지에 따라 피해 정도가 달라짐

AI에 대해 알려진 리스크와 알려지지 않은 리스크를 효율적으로 해결하기 위해서는;

사후적으로 리스크를 해결하려는 접근하기보다 AI 리스크 관리를 모든 기업 업무에 통합하여 관리의 연속성이 이루어질 수 있는 체계를 구축함으로써 '사전에 리스크를 통제하는 접근 방식'이 필요

AI 리스크 관리 필요성

데이터 유출 사고, 저작권 침해 등으로 인한 개인 및 기업 피해가 심각해짐에 따라 법 준수에 대한 사회적 요구가 크게 증가

- 개인정보보호법 개정을 통해 AI 규율 시도뿐만 아니라 개인정보 유출 사고, 데이터 불법 이용 등에 대한 제재 수준을 지속 강화
  - ❖ 개정 개인정보보호법(2024.3월 시행)은 AI 등 자동화된 결정에 대한 정보주체 권리 구체화(설명 또는 검토 요구, 거부권 부과), 개인정보보호책임자(CPO)의 자격 요건 강화 등

해외 주요국은 글로벌 AI 규범 확립을 주도하기 위해 자국 산업을 고려한 AI 입법을 추진 중

- 해외 주요국의 입법 방식이나 규제의 강도에는 차이가 있으나 AI 리스크 관리를 위한 사전 검증을 시행한다는 점에서 유사함
  - ❖ EU는 AI가 초래할 위험에 대한 포괄적 규제 원칙을, 미국은 자국 산업 보호 및 자율 규제 우선 원칙을 설정
- AI 안전성 평가 프레임워크 구축, AI 국제표준 인증 마련 등 AI 표준 및 국제 배포 방식에 대한 국제 협력도 활발해지고 있음

비즈니스 리스크 등 일부 AI 리스크가 법제도 위반 리스크에서 촉발된다는 점을 고려할 때;

우선적으로 기업에 적용되는 국내외 AI 법제에 대한 명확한 이해를 토대로 각국이 요구하는 수준에서 AI 리스크를 관리하여 법 위반 리스크를 최소화할 수 있는 체계를 수립하는 것이 필요

SHIN&KIM
법무법인(유) 세종

3. AI 거버넌스 관련 논의

AI 거버넌스 구현 시도 확대

전세계 최초 EU AI Act 제정(2024.3.13일) 등 전 세계적으로 AI 리스크를 심각하게 고려하는 정책 입안자의 관심이 증가, AI 부작용 및 사회적 비용 최소화를 위한 입법 시도가 빠르게 확산

- 각국은 개인정보보호 중심설계(Privacy by Design), Trust-by-design 접근, 안전성 평가, 영향평가, 신뢰성 검인증, 제3자 외부평가 등을 논의하며, AI 정책 수립 시 국제규범과의 일치화를 시도
- AI를 지원하는 기술 사양과 국제표준 등 표준화도 추진
  - ❖ 정보보호 및 개인정보 보호 관리체계(ISMS/ISMS-P), 정보보호 경영시스템(ISO 27001, 27701) 뿐만 아니라 AI 관련 국제적 인증 체계(ISO/IEC JTC 1/SC 42) ISO/IEC 42001 등

해외 주요국은 글로벌 AI 규범 확립을 주도하기 위해 자국 산업을 고려한 AI 입법을 추진 중

- 입법 방식이나 규제의 강도에는 차이가 있으나 AI 리스크 관리를 위한 AI 거버넌스 구축, 사전 검증 시행 등 유사 내용을 포함
- EU GDPR의 PbD, 미국 AI 행정명령의 Trust-by-design 등은 AI 상품/서비스 설계 단계에서부터 개인정보 보호, AI 신뢰 향상을 지향
  - ❖ EU는 AI가 초래할 위험에 대한 포괄적 규제 원칙을, 미국은 자국 산업 보호 및 자율 규제 우선 원칙을 설정

국내 역시 글로벌 차원에서 논의 중인 안전한 데이터 이전 규범에 대한 지속 모니터링 및 규범 논의에의 참여를 시도하고 있으며, 개인정보 보호법 2차 개정 등 통해 해외 주요국 법제도와의 상호운용성 확보 시도

AI 거버넌스 구현 시도 확대

전 세계적으로 AI 원칙, 프레임워크, 가이드라인 등 수립을 통해 AI 거버넌스 구현 관련 논의를 활발하게 진행 중

AI 원칙	AI 프레임워크	AI 법 및 정책	AI 가이드라인	AI 표준 및 인증
Guiding concepts and values	General operating structures, objectives, and definitions	Rules enacted and enforced by government	Practices, structures, and actions that are optional but encouraged	Sets of practices and controls that demonstrate compliance with laws or provide assurance
• OECD AI Principles • Asilomar AI Principles • IEEE's Ethically Aligned Design • Montreal Declaration for a Responsible Development of Artificial Intelligence	• NIST AI Risk Management Framework • OECD Framework for the Classification of AI systems	• AI Act (EU) • The Artificial Intelligence and Data Act (Canada) • NYC Local Law 144 of 2021 • American Data Privacy and Protection Act, Section 207 (US) • Internet Information Service Algorithm Recommendation Management Regulations (China)	• White House's voluntary commitments form leading AI companies • Canada's generative AI code of conduct	• ISO/IEC JTC 1/SC 42 • IEEE P7000 series of standards projects • CEN/CENELEC standards development • RAI Institute's Certification Program for AI Systems

자료: BCG analysis; Responsible AI Institute.

AI 거버넌스 정의

AI 리스크 최소화 및 비즈니스 혁신 창출을 위해서는 사후 리스크 대응보다 사전 리스크 관리가 필요, 이를 위해서는 개별 기업에 특화된, 신뢰할 수 있고 책임감 있는 AI 거버넌스의 선제적 구축이 필수

- 조직 내 AI 윤리 등 기본 원칙 및 내부 정책 가이드를 수립하는 것에 더해 기업 비즈니스 프로세스 전반에 걸쳐 AI의 잠재적 위험을 사전에 평가하고, 위험을 체계적으로 관리하기 위한 조직과 내부 절차가 필요
- AI 신뢰성 확보를 위한 국제적 요구사항을 반영하여 AI 도입 및 운영 과정에서 발생하는 리스크 선별, 분석, 대응, 평가를 할 수 있는 End-to-End 프로세스 도입 등 고려

AI 거버넌스

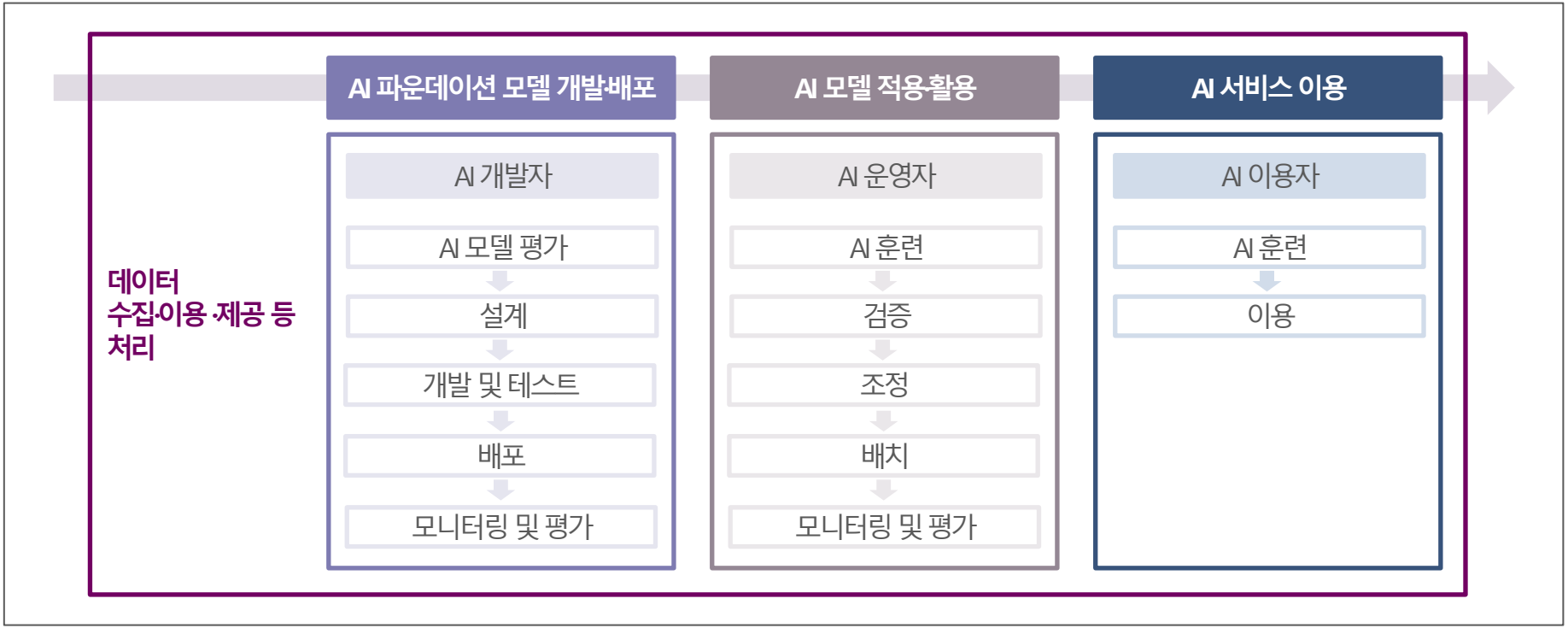
AI 라이프사이클에 대한 지속적 모니터링을 통해 각 단계별 발생 가능한 리스크를 식별하고, 해당 리스크 및 잠재적 영향을 최소화 및 제어할 수 있는 관리·감독 프레임워크를 의미

[AI 라이프사이클]

AI 파운데이션 모델 개발·배포 ▶ AI 모델 적용·활용 ▶ AI 서비스 이용

AI 거버넌스 정의

[참고: AI 라이프사이클]



AI 거버넌스 구현의 중요성

AI는 선택이 아닌 필수

혁신을 통한 생존

- AI를 **더 전사적으로 활용**할수록 업무 효율화, 생산성 향상, 고객 가치 혁신 등 경영적으로 얻을 수 있는 **효과는 더 극대화**
- AI 도입이 당장의 성과로 이어지지 않더라도 장기적 관점에서 **데이터 기반 예측 역량을 강화**할 경우 新 비즈니스 모델 개발을 통해 **더 큰 성과 창출**

AI의 양면성 극복

데이터 관련 근원적 취약점 존재

- 기업이 차별화된 서비스 제공을 위한 정확한 상황과 맥락을 파악하는데 **데이터 분석이 필수**
  → AI 활용 시 최우선적으로 고려되어야 할 것은 **다양한 데이터를 효율적으로 수집, 통합, 활성화, 관리할 수 있는 AI 거버넌스 구축 방안임**
- AI 악용, 데이터 유출, 확장 프로그램 취약성 등 상시 존재하는 보안 위협으로 인한 **비즈니스, 매출, 고객 손실 및 평판 손상 등 우려가 상당**

비즈니스 전반에 내재된 AI 리스크 통제

전사 차원의 사전 리스크 관리 필수

- AI 리스크 관리의 핵심은 AI 수명주기 동안의 **'지속적, 시기적절한 수행'**과 각각의 **'비즈니스 모델에 맞는 조정'**
- AI 리스크의 사후 관리는 비즈니스 모델, 데이터 보호, 평판, 법률 등 기업 프로세스 전반에 걸쳐 문제를 더욱 복잡하게 만드는 AI에 효과적으로 대응하는데 한계
  → **AI 모델 디자인 단계**에서부터 데이터 품질 관리, 데이터 관련 사고 예방 방안을 마련, 기업 특성 및 가치에 부합하는 **AI 리스크 사전 통제 체계**가 필요

SHIN&KIM
법무법인(유) 세종

4. AI 거버넌스 구현 위한 체크리스트

국내외 법제도 정합성 제고

개요

국내외 AI 법제에 대한 명확한 이해를 토대로 각국이 요구하는 수준에서의 AI 리스크 관리 및 최소한의 신뢰성 확보를 위한 내부 체계 수립

국내외 AI 법제 및 정책 모니터링, AI 국제 표준 및 인증 취득, 국내외 법제도 기반 리스크 자가점검

AI·데이터 관련 입법 및 정책 수립 동향 관련 모니터링을 통한 기업 내부 규제 라이브러리 구축

국내외 AI 법제가 요구하는 수준의 실시간 현황을 즉시 반영할 수 있는 규제 라이브러리 구축 통해 AI 법 위반 리스크 예방

- EU AI Act, 미국 정부의 AI 행정명령 등 해외 주요국의 관련 법령에 대한 구체적 분석
- PbD, Trust-by-design 접근, 안전성 평가, 영향평가, 신뢰성 검인증, 제3자 외부평가 등 국제 규범 수립 동향 모니터링

AI 관련 프레임워크, 국제표준 인증 등 AI 표준 및 국제 배포방식 준수

AI 위험 기반의 검증 항목 및 절차에 대한 표준화를 통해 기업 신뢰성 및 대외 이미지 제고, AI 리스크로 인한 손실 최소화

- ISMS/ISMS-P, ISO 27001, 27701, AI 관련 국제적 인증 체계(ISO/IEC JTC 1/SC 42), ISO/IEC 42001 등 AI 표준 및 인증 획득 등

맞춤형 AI 위험통제(Risk Management) 모델 체계 확립

개요

AI 라이프사이클 각 단계에 대한 주기적 모니터링 및 최신화된 국내외 규범 준수 여부 평가 절차 진행

비즈니스 단계별 AI 잠재적 위험 파악 → 맞춤형 AI 원칙 수립 → 감사체계 구축 → 위험 및 영향 평가 → 위험 관리방안 제시 → 주기적 모니터링 및 평가체계 제시

지속 가능한 AI 리스크 위험통제 원칙 수립

AI 리스크의 상시 평가를 통해 신규 제품·서비스 기획, 설계 및 출시 등 모든 단계에 적용 가능한 신뢰성·안전성을 담보

- 글로벌 차원에서 수립 중인 AI 규범을 종합적으로 고려한 내부 AI 윤리 등 기본 원칙 기반 정책서, 가이드라인 수립
- 비즈니스 프로세스 단계별 내부 통제장치(책임자 권한 및 책임)를 설정하는 기준 마련

기업 특성을 고려한 맞춤형 위험통제 모델 구축

기존 데이터 내지 새롭게 생성될 데이터에 대한 신뢰성, 정확성 등을 법제도적 관점에서 정량적으로 판단

- 데이터 수정, 변환, 통합 또는 재수집 과정에서 발생 가능한 비용 및 위험도를 사전에 객관적으로 평가

상시적 데이터 매니지먼트(Data management) 체계 활성화

개요

AI·데이터 처리 흐름(flow)에 대한 최신성이 반영될 수 있는 정확한 식별체계 구축

데이터 흐름 분석(데이터 인벤토리 및 우선순위 지정) → 데이터 리스크 프레임화(법률 및 규제 요구사항 파악) → 위험 평가(위협 요소 및 취약성 파악) → 위험 관리(위험 완화, 해결, 이전) → 모니터링 및 평가

기업이 보유한 데이터 인벤토리 및 우선순위 지정을 통한 데이터 처리 흐름(flow) 분석

데이터 리스크에 대한 체계적 관리로 침해, 유출 등 사고 발생 시 신속한 원인 분석을 통한 시의적절한 대응

- 분석 결과는 기업이 활용하고 있는 데이터 가치 산정 및 새로운 비즈니스 전략 수립을 위한 기초 자산으로 활용

주기적 테스트 및 모니터링과 즉각적 개선 체계 구축

데이터 프로세스 리엔지니어링을 통해 최적의 데이터 활용과 식별된 혹은 식별되지 않은 리스크 식별

- AI의 시장 배포 전 다양한 내/외부 테스트를 통한 적절한 조치 이행과 배포 후 데이터 흐름(flow)에 대한 지속 모니터링으로 취약점 및 사고, 새로운 위험 및 오용 경향성 등 파악으로 AI 리스크 발생 가능성 최소화


Q
A
SHIN&KIM
법무법인(유) 세종

SHIN&KIM
법무법인(유) 세종

감사합니다.

법무법인(유) 세종 ICT 그룹 / AI센터

장준영 변호사

T. 02 316 4985

E. jyojang@shinkim.com

서울시 종로구 종로3길 17 디타워 D2 23층 (우)03155
TEL: 02 316 4114 | FAX: 02 756 6226

www.shinkim.com

본 자료에 대한 저작권 등 모든 권리는 법무법인 세종 및 작성 전문가에게 속하므로, 사전 허락 없이 본 자료를 사용, 복제, 배포, 활용하거나 다른 법률 사무소 등 제3자에게 제공하는 것은 엄격히 금지됩니다. 본 자료와 관련하여 의문이 있으신 경우에는 법무법인 세종 또는 본 자료에 기재된 담당 변호사에게 연락하여 주시기 바랍니다.