

기업의 AI 전환을 완성하는 3가지 핵심 동력: AiNex

보안, 협업, 거버넌스를 통합한 AI 컨설팅 자동화 플랫폼



AgentForge

AI 전환의 딜레마: 높은 수요, 전문가 부족, 그리고 데이터 보안



수요 급증

AI 컨설팅 서비스 수요는 급증하고 있으나, 전문 인력이 매우 부족한 현실에 직면해 있습니다.



전문성 부족

성공적인 AI 도입은 단순한 기술 문제를 넘어 전략, 조직, 데이터, 거버넌스 등 전사적 관점의 접근을 요구합니다.



데이터 보안

컨설팅 과정에서 기업의 가장 민감한 데이터가 외부로 유출될 수 있다는 우려는 AI 전환의 가장 큰 걸림돌입니다.

AiNex: 기술, 협업, 거버넌스를 통합한 솔루션

AiNex는 기업이 직면한 AI 전환의 3대 과제를 해결하기 위해 3가지 핵심 동력을 기반으로 설계되었습니다.

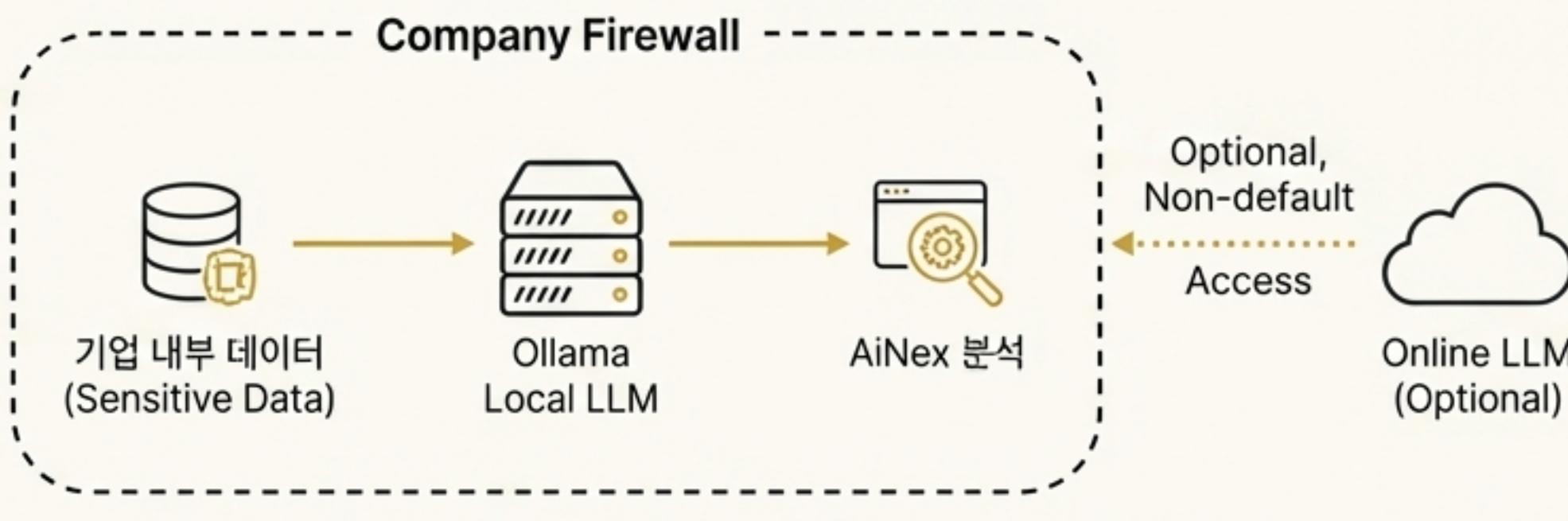


Pillar 1: 철저한 보안 아키텍처

데이터 유출 원천 차단: Local LLM 기반 하이브리드 아키텍처

Core Concept

AiNex의 설계 철학은 '보안 우선'입니다. Ollama(llama3.1:8b) 기반의 Local LLM을 기본으로 사용하여, 컨설팅 과정에서 기업의 민감 데이터가 외부 네트워크로 전송되는 것을 완벽하게 차단합니다.



```
# src/core/llm_provider.py
class LLMPProvider:
    def __init__(self, ...):
        self.model = model or settings.OLLAMA_MODEL # 'llama3.1:8b'
        self.base_url = base_url or settings.OLLAMA_BASE_URL # 'http://localhost:11434'
```

보안 요소	Local LLM	Online LLM
데이터 유출 위험	없음	존재
네트워크 의존성	없음	있음
네트워크 의존성	없음	있음
응답 지연	낮음	네트워크 상황 의존
비용	초기 설치비용	사용량 기반

5명의 전문 AI 에이전트, 하나의 팀처럼 협업하다

Strategy Analyst (전략 분석가)

AI 성숙도 진단 및 전략 로드맵 수립

Report Generator (보고서 생성기)

모든 분석 결과를 종합하여
경영진을 위한 최종 보고서 자동 생성

Use Case Designer (유스케이스 설계자)

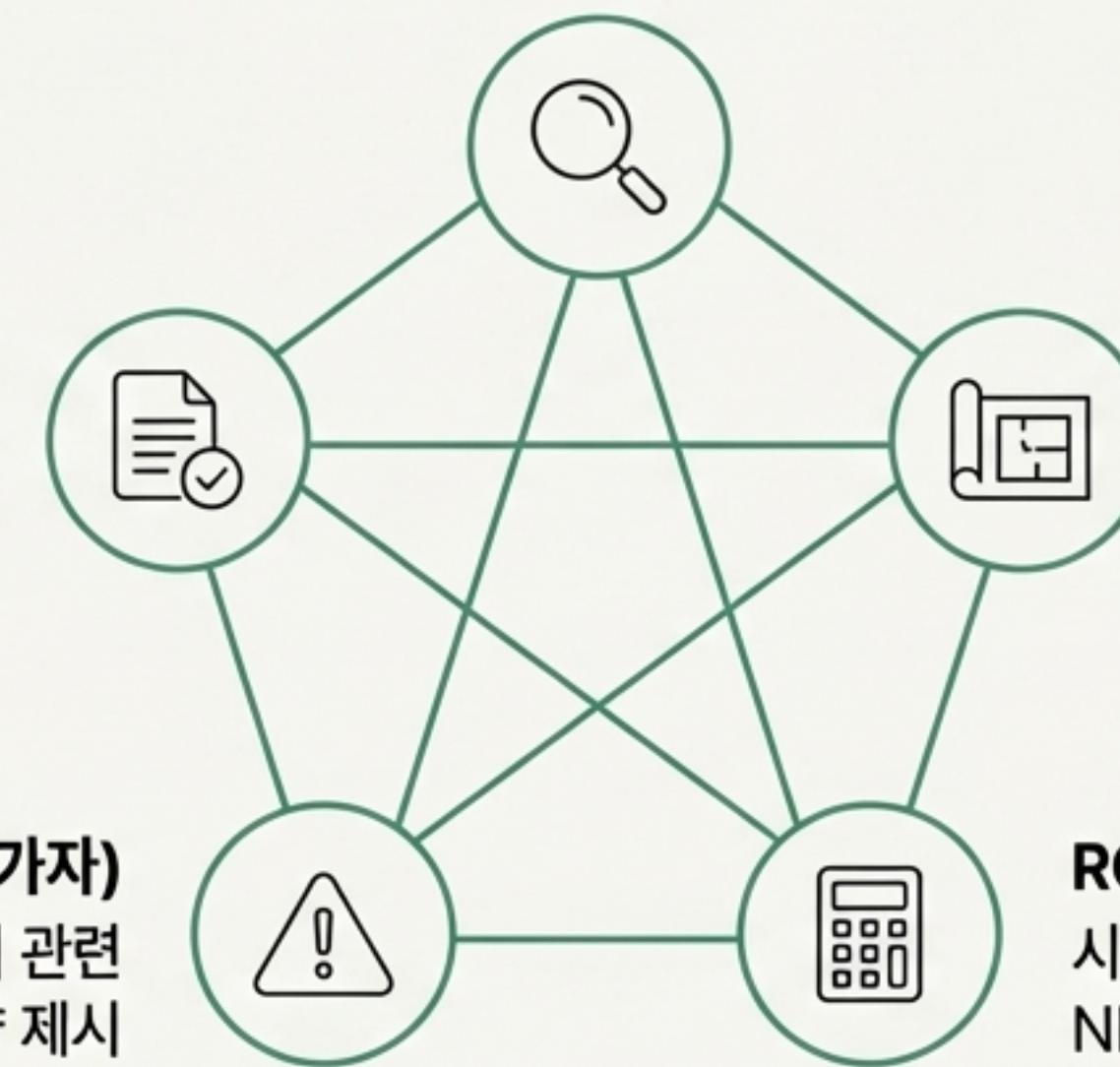
기업 특성에 맞는 AI 활용 사례
발굴 및 설계

Risk Assessor (리스크 평가자)

기술적, 조직적, 데이터 관련
리스크 식별 및 완화 전략 제시

ROI Analyst (ROI 분석가)

시나리오별 투자수익률(ROI), TCO,
NPV 등 정량적 기대 효과 분석



에이전트 메시 네트워크

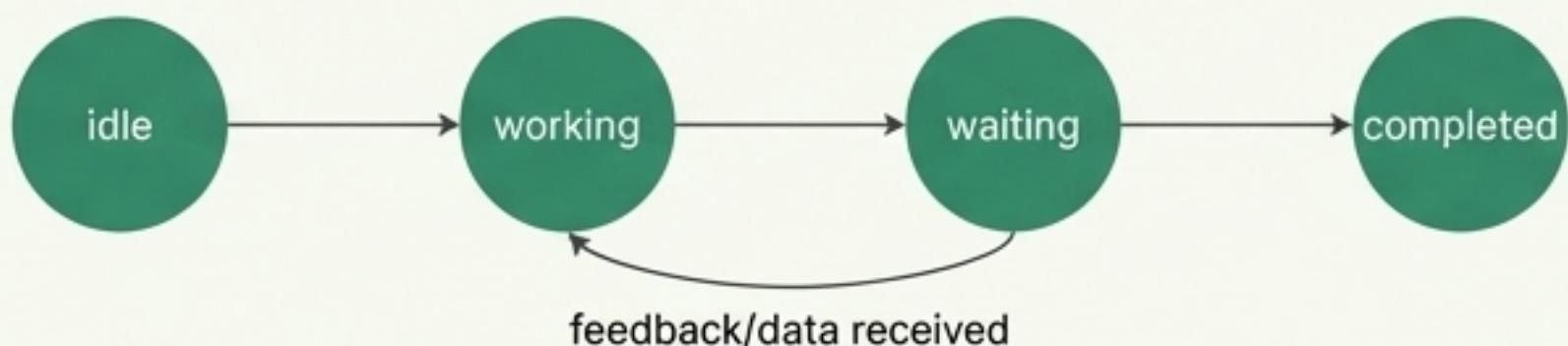
LangGraph 기반 오케스트레이션: 정교한 컨설팅 워크플로우 자동화

중앙 `ConsultingOrchestrator`가 LangGraph를 활용하여 에이전트들의 작업 순서, 상태, 데이터 흐름을 관리합니다. 이를 통해 복잡한 컨설팅 프로세스가 체계적으로 자동 실행됩니다.

워크플로우 상태 관리

```
class WorkflowState(TypedDict):
    # Key state fields
    maturity_assessment: Optional[Dict]
    scenarios: List[Dict]
    roi_analysis: Optional[Dict]
    risk_assessment: Optional[Dict]
    human_feedback: List[Dict] ←
    ...
```

인간 전문가의 개입 지점
(Point of human expert intervention)



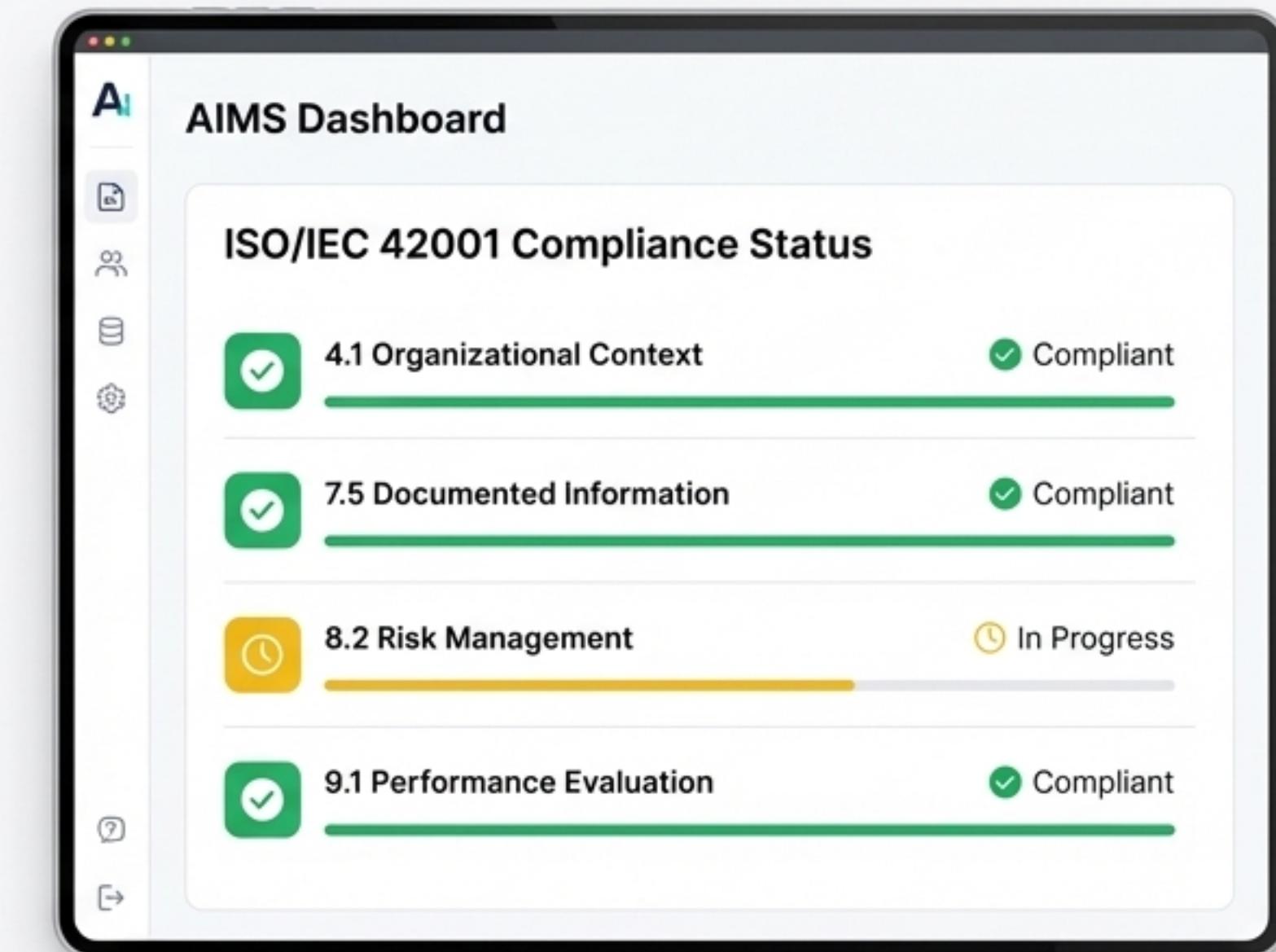
에이전트 메시지 프로토콜

메시지 유형	설명
`task`	특정 에이전트에게 작업 수행을 요청
`result`	작업 수행 결과를 다른 에이전트에게 전달
`feedback`	인간 전문가의 피드백을 워크플로우에 반영
`approval_request`	주요 결정(시나리오 선택 등)에 대한 인간의 승인 요청

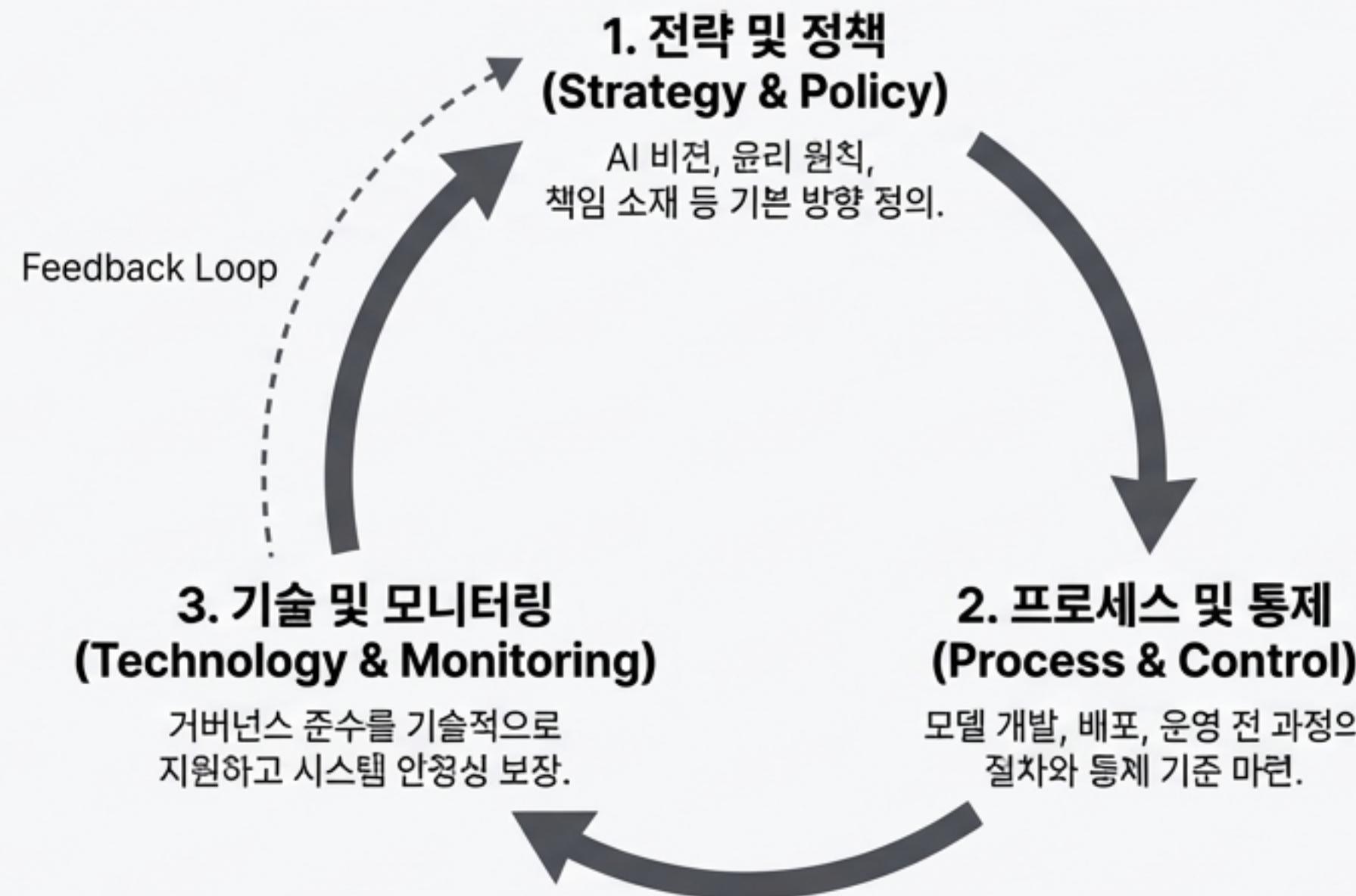
신뢰할 수 있는 AI를 위한 선택: ISO 42001 AIMS 프레임워크 내재화

AiNex는 AI 경영시스템 국제 표준인 ISO/IEC 42001의 요구사항을 플랫폼 기능과 직접 매핑한 'AIMS 대시보드'를 제공합니다. 이를 통해 조직은 AI 시스템의 규제 준수 현황을 실시간으로 파악하고 체계적으로 관리할 수 있습니다.

ISO 42001 조항 (Clause)	AiNex 플랫폼 기능/모듈 (Platform Feature/Module)
4.1 조직 상황 (Organizational Context)	Stage 1: AI 성숙도 진단 (AI Maturity Assessment)
7.5 문서화된 정보 (Documented Info)	자동 생성: 모델 카드, 데이터 시트 (Auto-generation: Model Card, Data Sheet)
8.2-8.3 위험 관리 (Risk Management)	AI 위험 등록부 (AI Risk Register)
9.1 성과 평가 (Performance Eval.)	Stage 5: 운영 및 모니터링 대시보드 (Operations & Monitoring Dashboard)



AI 거버넌스의 3대 핵심 영역: 전략, 프로세스, 기술의 통합 관리

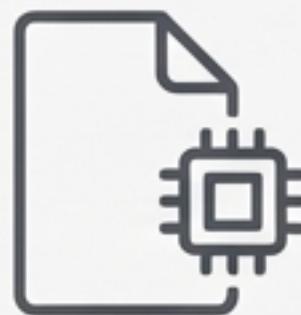


AiNex는 이 3대 영역이 유기적으로 연동되도록 지원합니다.

모니터링 결과(기술)는 정책 개선(전략)에 활용되고, 정책(전략)은 개발 및 배포(프로세스)에 반영됩니다.

투명성과 책임성 확보: 자동으로 생성되는 거버넌스 산출물

AiNex는 컨설팅 워크플로우 전 과정에서 수집된 데이터를 바탕으로 ISO 42001이 요구하는 핵심 거버넌스 문서를 자동으로 생성합니다.



Model Card

모델 카드 (Model Card)

모델의 성능, 제한사항, 편향성, 권장 사용 범위를 명시하여 투명성을 확보하고 오용을 방지합니다.



Data Sheet

데이터 시트 (Data Sheet)

학습 데이터의 출처, 구성, 품질, 개인정보 포함 여부를 문서화하여 데이터의 신뢰성과 적법성을 보장합니다.



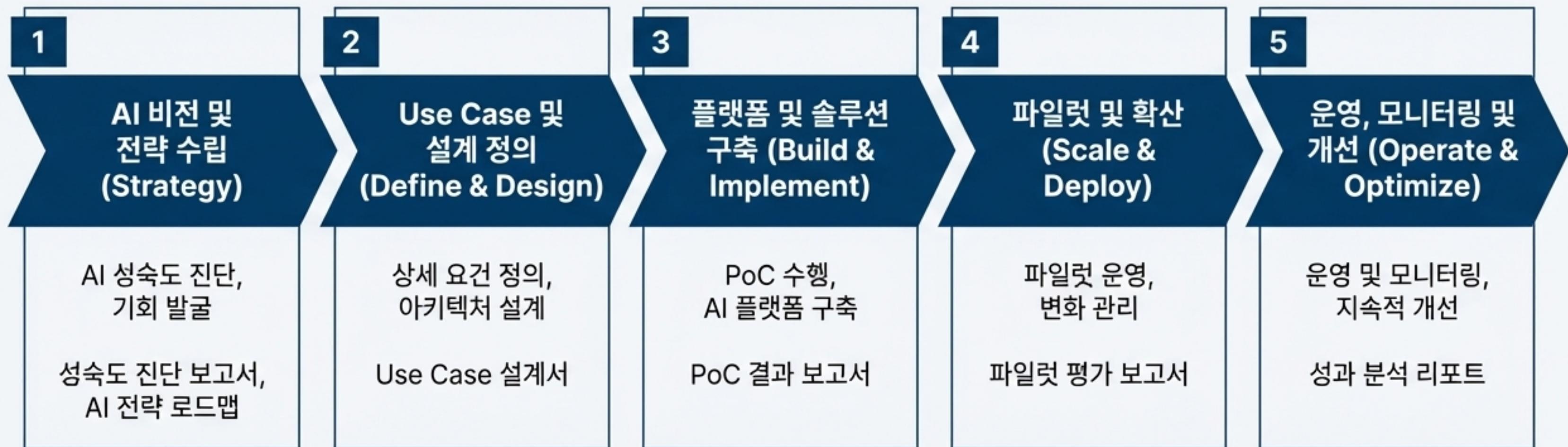
Risk Register

AI 위험 등록부 (AI Risk Register)

AI 시스템과 관련된 모든 기술적, 윤리적 위험을 식별, 평가, 추적하여 체계적인 위험 관리를 지원합니다.

아이디어에서 최종 보고서까지: 5단계 컨설팅 프레임워크 자동화

5단계 컨설팅 프레임워크 자동화



데이터 기반 의사결정: 정량적 분석과 가중치 시스템

AiNex는 컨설턴트가 입력한 기업 프로필 데이터를 기반으로 AI 성숙도, Use Case 적합도, 리스크를 정량적으로 평가하여 객관적인 의사결정을 지원합니다.



AI 성숙도 점수 (AI Maturity Score)

경영진 지원, 데이터 거버넌스, AI 경험 등 핵심 요소에 가중치를 부여하여 점수를 계산합니다.

$$\begin{aligned} \text{전략 점수} &= 2.0 \text{ (기본)} \\ &+ 1.0 \text{ (경영진 지원 } \geq 4) + \\ &+ 0.5 \text{ (AI 투자 예산 } > 0) \end{aligned}$$



Use Case 적합도 점수 (Use Case Fit Score)

데이터 가용성, 인프라 준비도, 인력 역량 등을 종합하여 Use Case의 성공 가능성을 평가합니다.

$$\begin{aligned} \text{적합도} &= 50 \text{ (기본)} \\ &+ 10 \text{ (데이터 품질 } \geq 3) + \\ &+ 10 \text{ (클라우드 보유)} \end{aligned}$$



시나리오 종합 점수 (Overall Scenario Score)

최종 시나리오 평가는 기대 수익(ROI)과 잠재 리스크를 균형 있게 고려하여 이루어집니다.

$$\begin{aligned} \text{시나리오 종합 점수} &= \\ &(ROI \text{ 점수} \times 0.6) \\ &+ (\text{리스크 점수} \times 0.4) \end{aligned}$$

3가지 시나리오 분석을 통한 최적의 AI 도입 전략 제안

AiNex는 기업의 예산, 리스크 수용도, 전략적 목표를 고려하여 세 가지 AI 도입 시나리오를 자동으로 생성하고, 각 시나리오의 장단점을 비교 분석하여 최적의 의사 결정을 지원합니다.

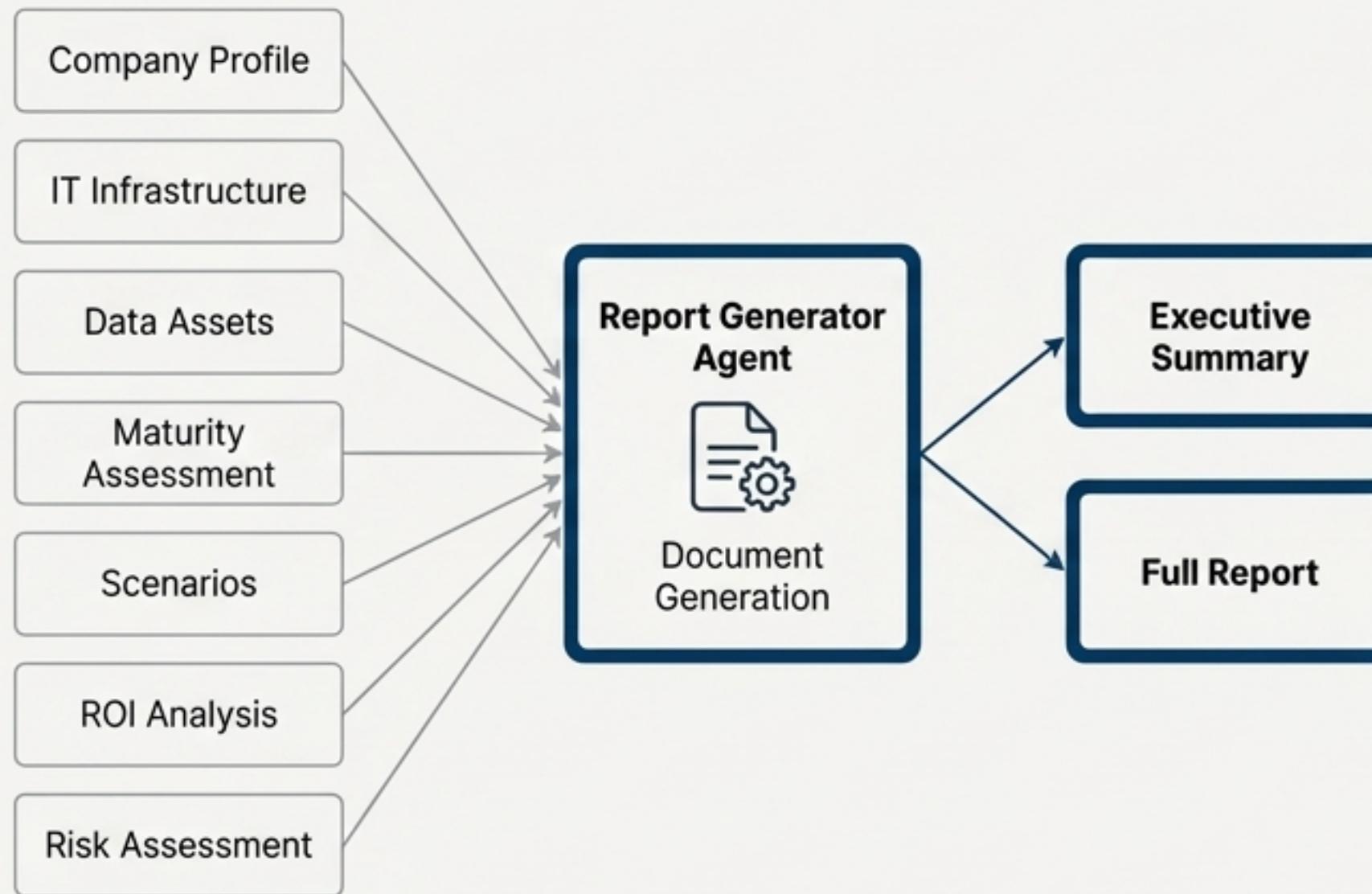
구분	보수적 시나리오 (Conservative)	균형 시나리오 (Balanced)	적극적 시나리오 (Aggressive)
핵심 초점 (Focus)	Quick Win 과제 집중	단기 성과와 중기 역량 구축 병행	비즈니스 혁신 및 전사 확산
예산 비율 (Budget Ratio)	60%	100%	150%
리스크 수용도 (Risk Appetite)	Low	Medium	High
예상 기간 (Timeline)	18 개월	24 개월	36 개월
종합 점수 (Overall Score)	7.8	8.5	8.1



모든 분석의 결정체: 경영진을 위한 종합 컨설팅 리포트

Report Generator 에이전트는 Strategy, Designer, ROI, Risk 에이전트의 모든 분석 결과를 취합하여, 경영진을 위한 Executive Summary와 실무자를 위한 상세 보고서를 자동으로 생성합니다.

Input to Output Flow



최종 보고서 구조 (Final Report Structure)

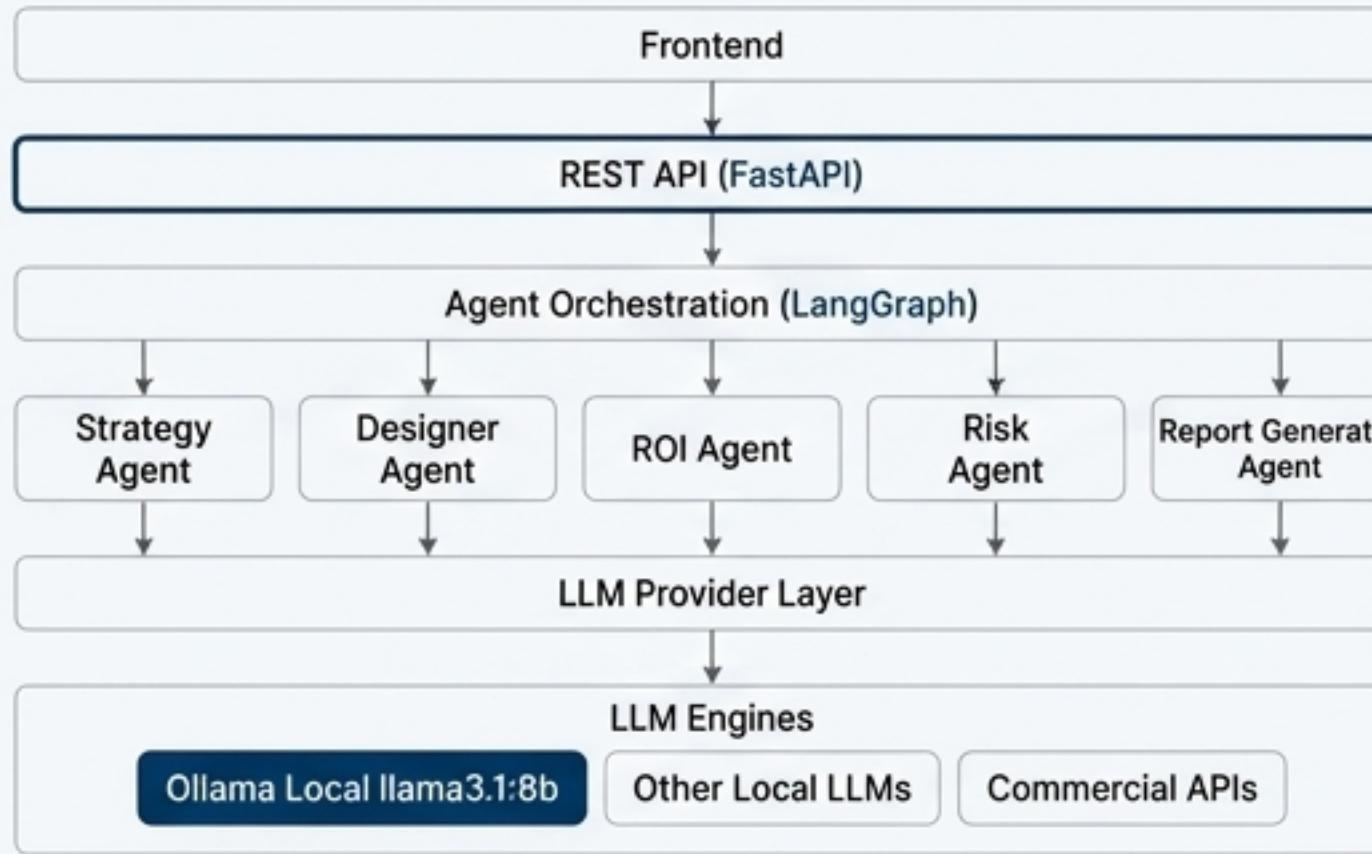
Executive Summary

- 1. 프로젝트 개요 (Overview)
- 2. AI 성숙도 진단 결과 (Maturity Assessment)
- 3. 시나리오 분석 (Scenario Analysis)
- 4. 권고사항 및 Next Steps (Recommendations)

Full Report

- Chapter 1: 개요 (Overview)
- Chapter 2: 현황 분석 (As-Is Analysis)
- Chapter 3: AI 전략 수립 (AI Strategy)
- Chapter 4: 실행 계획 (Execution Plan)
- Chapter 5: 기대 효과 (Expected Benefits)
- Chapter 6: 리스크 관리 (Risk Management)

AiNex 기술 아키텍처: 보안, 확장성, 그리고 전문성



계층 (Layer)	기술 스택 (Technology Stack)	핵심 역할 (Core Role)
Backend	FastAPI (Python 3.12)	고성능 REST API 서버
LLM Engine	Ollama (llama3.1:8b)	보안 중심의 로컬 LLM 추론
Agent Framework	LangChain, LangGraph	에이전트 워크플로우 오케스트레이션
Multi-Agent	CrewAI, AutoGen	역할 기반 AI 에이전트 협업
Database	SQLite + aiosqlite	비동기 데이터 저장 및 관리

오픈소스 기반의 최신 기술 스택을 활용하여 특정 벤더에 종속되지 않는 유연하고 확장 가능한 아키텍처를 구현했습니다.

인간 전문가와 AI의 협업: AI 전환의 새로운 표준을 제시합니다

“AiNex의 목표는 인간 컨설턴트의 전략적 통찰력과 AI의 정밀한 분석 능력을 결합하여, 더 빠르고, 더 정확하며, 더 신뢰할 수 있는 고품질 AI 컨설팅 서비스를 제공하는 것입니다.”

- **For Consultants**

컨설팅 업무 자동화로 핵심 전략 수립에 집중

- **For Companies**

전문가 부족 문제를 해결하고 데이터 기반의 객관적 의사결정 지원

- **For Everyone**

내재화된 거버넌스를 통해 책임감 있고 신뢰할 수 있는 AI 도입 실현

