pwc 삼일회계법인

AI가 바꾸는 자산운용업 거버넌스: 운영구조 변화와 대응전략

삼일PwC경영연구원 I Industry Focus
June 2026

들어가며

자산운용업에서의 경쟁력은 오랫동안 정보 해석의 속도와 판단의 정교함에 의해 결정되어 왔다. 최근에는 이러한 경쟁의 중심에 인공지능(AI)이 빠르게 편입되며, 리서치, 데이터 분석, 포트폴리오 관리, 리포팅 등에 이르기까지 AI 활용이 전방위적으로 확산되고 있다. 특히 AI의 등장 이후에는 업무 효율화를 넘어, 투자 의사결정에 실질적인 영향을 미치는 단계로까지 활용 범위가 확대되는 흐름이 나타나고 있다.

그러나 국내 자산운용업의 AI 도입은 전사 차원의 통합 전략에 따라 일관되게 추진되기보다 현업 부서 중심의 업무 효율화 수요에 따라 개별적으로 확산되어 온 측면이 있다. 이에 따라 AI 활용 범위는 빠르게 확대되고 있는 반면, 이를 통합적으로 관리할 전사적 통제 체계와 책임 구조는 아직 충분히 정립되지 못한 경우도 존재한다.

이에 따라 AI가 생성한 분석 결과와 정보가 실제 투자 판단 과정에 활용되는 비중이 높아질수록, 해당 결과에 대한 검증 절차와 책임 소재를 어떻게 관리할 것인지가 새로운 관리 이슈로 부상하고 있다. 이는 자산운용업의 핵심인 책임 있는 투자 판단과 내부통제 체계에도 직접적인 영향을 미칠 수 있다.

본 보고서는 이러한 문제 인식을 바탕으로, 자산운용업에서의 AI 도입이 야기하는 주요 리스크를 구조적으로 정리하고, 이를 효과적으로 통제하기 위한 AI 거버넌스의 설계 방향을 제시하는 데 목적이 있다. 다만 본 보고서는 자산운용업 가운데 집합투자업과 투자자문업, 투자일임업권을 중심으로 AI 활용에 따른 주요 이슈와 대응 방향을 살펴보는 데 초점을 두었다.

본 보고서는 전사적 관점에서의 통제 체계와 의사결정 및 책임 구조, 데이터 및 보안 관리 측면에서 자산운용사가 고려해야 할 핵심 요소를 중심으로 실질적인 적용 가능성을 갖는 거버넌스 프레임을 제안하고자 한다.

Contents

01

AI 확산은 자산운용업의 운영 환경을 어떻게 변화시키고 있는가

1.1 AI는 자산운용업의 통제 체계를 어떻게 바꾸고 있는가

AI는 금융사의 업무 생산성을 높이고 있으나, 인간 중심의 책임 체계와 내부통제 체계 전반에 새로운 과제를 야기

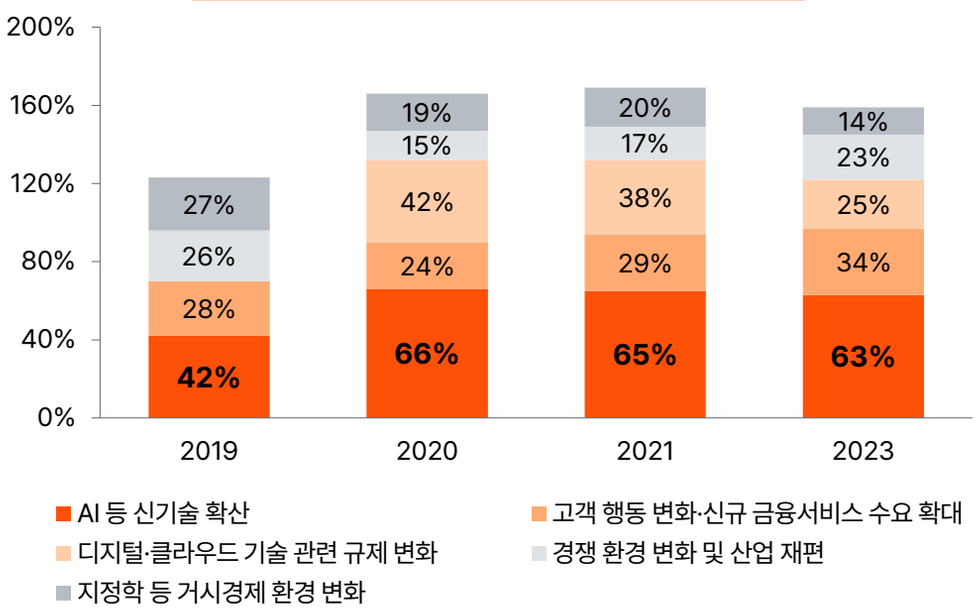
최근 금융산업 전반에서는 AI 기술의 발전과 함께 업무 운영 방식과 의사결정 구조 전반에 걸쳐 변화가 빠르게 나타나고 있다. 초기의 AI 활용이 정형 데이터 기반의 분석 · 예측 기능이나 반복 업무 자동화 중심이었다면, 최근에는 정보 검색 · 요약, 문서 작성, 질의 응답, 데이터 분석 지원 등 다양한 업무 영역으로 활용 범위가 확대되고 있다. 특히 대규모 언어모델(Large Language Model, LLM)을 포함한 AI 기술의 발전은 금융회사가 복잡한 데이터와 정보를 보다 빠르게 해석하고 활용할 수 있는 환경을 제공하면서, 기존 업무 수행 방식 자체에 변화를 가져오고 있다.

금융산업은 본질적으로 방대한 정보와 데이터의 수집 · 분석 · 활용을 기반으로 운영되는 산업이라는 점에서 AI 활용 수요가 높게 나타나는 분야 중 하나이다. 리서치, 고객 응대, 상품 설명, 리스크 관리, 내부통제, 컴플라이언스, 보고 및 문서 작성 등 다양한 업무에서 정보 처리의 속도와 정확성이 중요한 경쟁 요소로 작용해 왔으며, AI는 이러한 업무의 효율성과 생산성을 높일 수 있는 수단으로 빠르게 확산되고 있다.

이와 함께 AI 기술의 발전은 금융산업 내 정보 처리와 의사결정 지원 방식에도 변화를 가져오고 있다. 반복 업무를 자동화하는 수준을 넘어, AI가 데이터를 해석하고 요약하며 일정 수준의 분석 결과와 실행 방향까지 제시하는 형태로 발전하면서, 업무 수행 과정에서 AI가 담당하는 역할과 영향 범위 역시 빠르게 확대되고 있다.

글로벌 금융기관 경영진이 선정한 금융산업 주요 변화 트렌드

글로벌 금융기관 경영진들은 향후 몇 년간 금융산업에 가장 큰 영향을 미칠 요인으로 **AI 등 신기술**New Technologies을 지목



자료: Economist Impact, Temenos, Statista, 삼일PwC경영연구원 재구성
주석: 해당 설문조사는 전 세계 글로벌 금융기관 경영진 300명을 대상으로 시행

AI의 업무 내재화에 따른 위험관리·통제 체계 중요성 증대와 AI 거버넌스 역량 확보 필요성 확대

최근에는 여러 업무 단계를 연속적으로 수행하거나 외부 시스템과 연동해 작업을 실행하는 에이전틱 AI(Agentic AI) 형태의 기술도 확산되고 있으며, 이는 향후 AI가 실제 업무 흐름과 의사결정 과정에 보다 깊게 개입할 가능성을 보여주고 있다.

이러한 변화는 금융회사 전반의 업무 운영 방식과 정보 처리 구조에도 영향을 미치고 있다. 특히 생성형 AI와 에이전틱 AI는 여러 업무 단계와 시스템을 연결하는 형태로 활용되면서 업무 수행 과정과 정보 흐름 구조를 더욱 복잡하게 만들고 있다. 이와 같은 변화는 자산운용업의 생산성과 경쟁력을 높이는 긍정적인 요인으로 작용하는 동시에 기존 운영 방식과 내부통제 체계 측면에서 새로운 과제를 제기하고 있다.

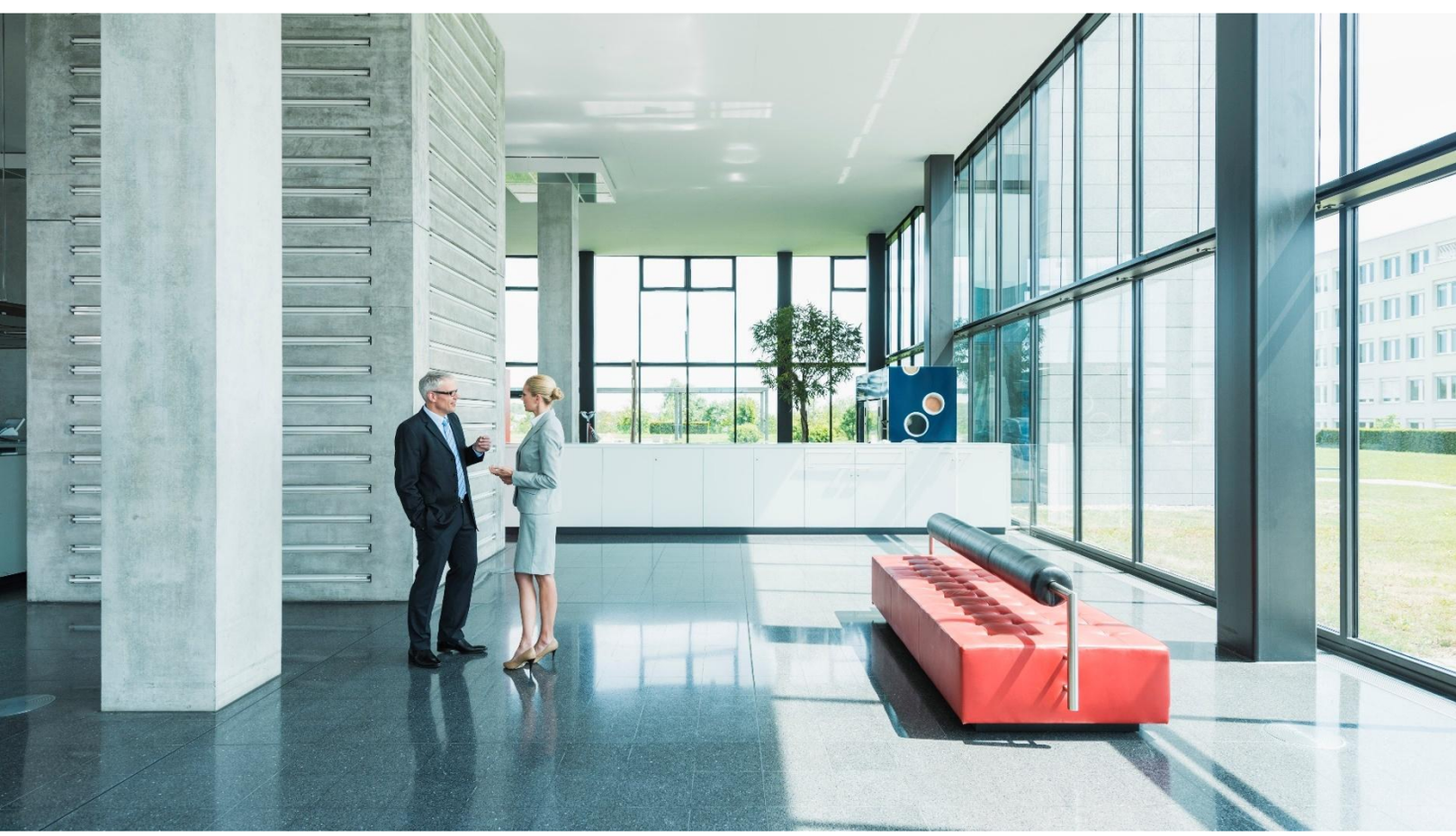
반면 AI 활용에 대한 검토·승인 기준과 책임 체계, 통제 원칙은 아직 충분히 정립되지 못한 경우도 존재하며, 기술 도입 속도에 비해 관리 체계 정비가 뒤따르지 못하는 모습도 나타나고 있다. 그 결과 기존 내부통제 체계만으로는 AI 활용 과정에서 발생하는 책임 소재와 검증 절차, 권한 통제 등을 충분히 관리하기 어려워지고 있으며, 새로운 관리 원칙과 통제 체계 정비의 필요성도 함께 커지고 있다. 특히 자산운용업은 고객 자산을 운용하며 투자 의사결정을 수행하는 산업이라는 점에서, AI 활용에 대한 적절한 검증과 통제가 이루어지지 않을 경우 투자 판단의 적정성과 내부통제 체계 측면에서 새로운 리스크가 발생할 수 있다.

이러한 문제의식은 최근 AI 규제 환경 변화 속에서도 점차 중요하게 다뤄지고 있다. 최근 규제 환경 역시 AI 활용 자체보다 AI 활용 과정에 대한 위험관리와 책임 체계 확보를 요구하는 방향으로 발전하고 있다. 이러한 변화는 AI 활용 과정에 대한 책임성과 통제 가능성을 확보해야 하는 거버넌스 이슈로 점차 확대되고 있다. 향후 자산운용업에서는 AI 활용 확대와 함께, 이를 안정적으로 관리 · 통제하고 인간 중심의 책임 체계를 유지할 수 있는 거버넌스 역량 확보가 핵심 과제로 부상할 가능성이 높다. 이에 따라 AI 활용 과정 전반에 대한 관리 기준과 책임 체계, 검토 · 승인 절차 등을 통합적으로 운영할 수 있는 거버넌스 체계의 필요성 역시 커지고 있다.

본 보고서는 이러한 환경 변화를 배경으로, 자산운용업에서의 AI 도입 현황과 그에 따른 주요 리스크를 구조적으로 점검하고, 이를 효과적으로 관리하기 위한 AI 거버넌스의 설계 방향을 제시하는 데 목적이 있다. 특히 의사결정 및 책임 체계, 통제 및 모니터링 체계, 데이터 및 보안 관리 측면에서 자산운용사가 고려해야 할 핵심 요소를 중심으로 거버넌스 구축 방향을 제시하고자 한다.

02

자산운용업의 AI 활용 확대와 내부통제의 구조 변화



2.1 자산운용업의 AI 도입 확산 배경

AI 기반 정보 분석 역량 강화와 투자 의사결정 경쟁 심화가 자산운용업의 AI 도입 확대를 이끄는 핵심 배경으로 작용

국내 자산운용업은 시장과 산업, 기업에 대한 정보를 빠르게 해석하고 투자 판단으로 연결하는 것이 핵심 경쟁력이라는 점에서 AI 활용 수요가 높은 분야 중 하나이다. 자산운용사는 거시경제 지표와 기업 공시, 시장 데이터, 뉴스 · 리서치 자료, 대체데이터 등 방대한 정보를 기반으로 투자 의사결정을 수행하며, 정보 분석 속도와 해석 역량이 운용 성과와 직결되는 특성을 가진다.

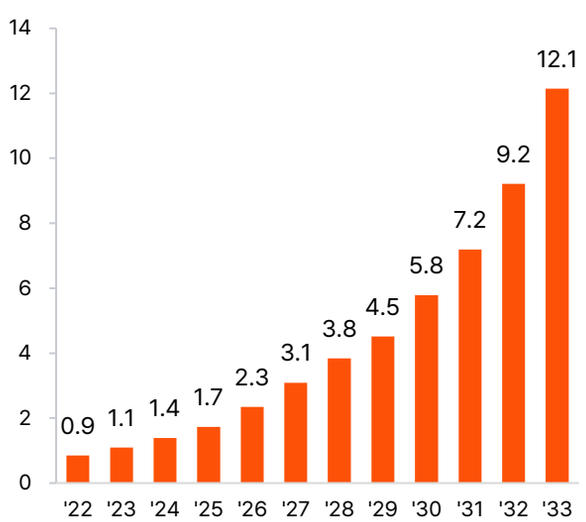
최근 금융시장 변동성이 확대되고 투자 환경의 불확실성이 높아지면서 보다 신속하고 정교한 데이터 분석 체계에 대한 수요가 확대되고 있다. 이에 따라 국내 자산운용사들 역시 업무 효율성과 정보 처리 역량 강화를 위해 AI 도입을 빠르게 확대하고 있다.

이와 함께 자산운용사가 자체적으로 AI 모델을 직접 개발하지 않더라도, 생성형 AI 기반 서비스와 서비스형 소프트웨어(Software as a Service, SaaS) 업무 도구를 활용해 과거보다 훨씬 낮은 비용과 진입 장벽으로 AI 기능을 도입할 수 있는 환경 역시 빠르게 조성되고 있다.

또한 자산운용업은 프론트 조직의 속도와 자율성이 강하게 작동하는 산업이라는 점에서도 AI 도입 유인이 크다. 시장 변화에 대한 신속한 대응과 정보 해석 능력이 중요한 만큼, 현업 조직은 반복적인 자료 탐색과 데이터 정리, 리서치 업무를 줄이고 보다 고차원의 투자 판단에 집중할 수 있는 환경을 요구하고 있다. 최근에는 생성형 AI와 에이전틱 AI 기반 기술 확산으로 인해 자산운용사의 업무 운영 구조 역시 점차 자동화·연결형 구조로 변화하고 있다.

이러한 변화는 실제 AI 활용 범위의 확대와 현업 조직 전반으로의 확산으로도 이어지고 있다. 과거에는 대형 운용사와 일부 전문 조직 중심으로 AI 활용이 제한적으로 이루어졌다면, 최근에는 운용역과 리서치 조직, 마케팅·지원 부서 등 현업 전반으로 AI 활용이 확산되는 양상도 나타나고 있다. 이는 중소형 운용사를 포함한 다양한 사업자들이 제한된 인력과 비용 구조 안에서도 업무 효율성과 생산성을 높일 수 있는 수단으로 AI를 적극 검토하게 만드는 배경이 되고 있다.

글로벌 금융산업 내 생성형 AI 시장 규모 전망 (십억 달러)



자료: MarketResearch.biz, Statista, 삼일PwC경영연구원 재구성

자산운용업의 AI 도입 주요 동인

1	정보 해석 · 분석 기반 운용 경쟁력 강화
2	AI 기반 투자 판단 및 의사결정 지원 확대
3	시장 대응 속도 및 실시간 분석 역량 강화
4	리서치 · 정보 탐색 업무 효율화
5	반복 · 비정형 업무 자동화 확대
6	제한된 인력 구조 내 생산성 · 비용 효율성 확보

자료: 삼일PwC경영연구원

2.2 자산운용업의 AI 활용 범위

AI 확산에 따라 리서치·투자·리스크 관리 및 컴플라이언스 등 핵심 업무 전반으로 AI 활용 범위가 확대되는 추세

최근 자산운용업에서는 AI가 일부 실험적 기능을 넘어 실제 업무 과정 전반으로 빠르게 확산되고 있다. 특히 생성형 AI와 대규모 언어모델(LLM) 기반 서비스 확산은 기존 정형 데이터 중심의 분석을 넘어, 비정형 정보 해석과 문서 기반 업무까지 AI 활용 범위를 확대시키고 있다. 이에 따라 AI 활용은 실제 현업 업무 과정 전반으로 빠르게 확산되고 있다.

우선 리서치와 정보 분석 영역에서는 AI 활용이 빠르게 확대되고 있다. 최근에는 AI를 활용해 대량의 시장 정보와 대안 데이터를 신속하게 요약 · 정리하고 핵심 이슈를 추출하거나, 특정 산업 · 기업 관련 변화 흐름을 비교 · 분석하는 방식의 활용이 증가하고 있다. 또한 기업 실적 발표와 컨퍼런스콜, 정책 발표문, 시장 뉴스 등 비정형 텍스트 기반 정보를 분석해 투자 판단에 필요한 핵심 내용을 정리 · 비교하는 활용 역시 점차 본격화되고 있다.

이 과정에서 AI는 정보 간 연관성 분석과 핵심 이슈 정리, 비교 · 요약 업무까지 지원하는 형태로 활용 수준이 고도화되고 있다.

비정형 데이터 분석과 자연어 기반 업무 자동화 확산에 따라 자산운용업의 업무 수행 방식 및 정보 처리 구조 변화 가속화

투자 판단 지원 영역에서도 AI 적용 사례가 증가하고 있다. AI는 대규모 데이터 분석과 패턴 탐지를 기반으로 시장 흐름 및 투자 관련 정보를 정리 · 분석하는 방식으로 활용되고 있으며, 글로벌 선진 금융사와 일부 대형 운용사를 중심으로 투자 전략 검토와 포트폴리오 운영 지원, 시장 시그널 탐지 등 다양한 방식의 활용이 이루어지고 있다.

예를 들어 특정 산업이나 자산군 관련 시장 흐름을 분석하거나, 거시경제 변수 변화에 따른 시나리오를 정리하고 투자 아이디어 검토를 지원하는 방식의 활용이 이루어지고 있다. 또한 일부 영역에서는 AI를 활용해 포트폴리오 위험 요인을 사전에 탐지하거나, 운용 과정에서 발생할 수 있는 이상 징후를 모니터링하는 시도도 나타나고 있다. 다만 현재 국내 자산운용업에서는 AI가 인간의 투자 판단을 직접 대체하기보다, 운용 인력의 의사결정을 지원하는 보조 수단 형태로 사용되는 경우가 많은 상황이다.

리스크 관리와 컴플라이언스 영역에서도 AI 활용 범위가 확대되고 있다. 이상 거래 탐지, 시장 모니터링, 규제 · 공시 사항 점검, 내부 보고 지원 등 반복적이고 데이터 집약적인 업무를 중심으로 AI 사용이 증가하고 있으며, 이를 통해 모니터링 범위와 업무 처리 속도를 동시에 확대하려는 움직임이 나타나고 있다.

특히 금융규제와 공시 요구사항이 지속적으로 증가하는 환경에서 AI를 활용해 규제 변경사항을 정리하거나, 내부 보고 및 문서 작성 업무를 지원하는 사례도 늘어나고 있다. 또한 고객 응대 기록과 운용 관련 보고서, 내부 커뮤니케이션 자료 등을 분석해 리스크 징후 탐지와 준법 점검 등을 지원하려는 시도 역시 점차 확대되고 있다.

후선 업무와 운영 지원 영역에서도 AI 활용은 빠르게 확산되고 있다. 보고서 작성, 회의록 정리, 데이터 정리 및 문서화, 프레젠테이션 초안 작성 등 반복적이고 비정형적인 문서 업무에서 AI 기반 자동화 도구 사용이 증가하고 있으며, 이를 통해 실무 인력의 업무 부담을 줄이려는 시도가 이어지고 있다. 특히 최근에는 자연어 기반 인터페이스 확산으로 인해 비전문 인력 역시 비교적 손쉽게 AI 기능을 활용할 수 있는 환경이 조성되면서, 과거 일부 기술 조직 중심이었던 AI 활용이 현업 조직 전반으로 빠르게 확산되는 흐름도 나타나고 있다.

자산운용업의 AI 활용 Case

리서치 · 정보분석	• **시장정보 요약 · 정리:** 시장 뉴스, 기업 공시, 산업 보고서, 애널리스트 자료, 거시경제 데이터 등의 신속한 요약 · 정리 및 핵심 이슈 추출 • **산업 · 기업 변화 분석:** 산업 · 기업 관련 시장 변화와 경쟁 환경, 정책 변화 분석 및 투자 아이디어 검토 지원 • **비정형 텍스트 분석:** 기업 실적 발표문, 컨퍼런스콜, 정책 발표문, 시장 뉴스 등 비정형 정보 기반 핵심 내용 및 변화 흐름 분석
투자 판단 지원	• **시장 흐름 · 투자 시그널 분석:** 대규모 데이터 기반 시장 흐름 및 투자 관련 정보 분석, 자산군 · 산업군 변화와 투자 시그널 탐지 • **시나리오 분석:** 금리 · 환율 등 거시경제 변수 기반 시장 시나리오 예측 및 투자 전략 검토 지원 • **포트폴리오 · 투자 아이디어 분석:** 포트폴리오 위험 요인과 자산 간 관계 분석, 투자 아이디어 관련 시장 데이터 비교 · 정리
리스크 관리	• **이상 거래 · 위험 신호 탐지:** 이상 거래 및 포트폴리오 위험 요인을 사전에 탐지하고, 비정상적 거래 흐름 · 급격한 변동성 확대 · 특정 자산군 쏠림 현상 · 이상 패턴 등을 실시간 모니터링 • **실시간 위험 모니터링:** 시장 변동성과 운용 현황을 실시간으로 모니터링하고, 주요 위험 요인 변화 상황과 포트폴리오 영향도를 자동 정리 · 보고하며 위험 경보 체계 운영 지원
업무 자동화	• **협업 · 문서 업무 지원:** 회의록 정리, 이메일 초안 작성, 내부 커뮤니케이션 자료 생성 등 반복적 협업 · 문서 업무 자동화 지원 • **업무 연계 · 알림 자동화:** 시장 변화와 주요 이벤트 발생 시 실시간 알림 제공, 보고 · 공유 · 후속 업무 연계 등 업무 흐름 자동화 지원
준법 · 컴플라이언스	• **규제 · 공시 대응 지원:** 금융규제 및 공시 요구사항 변화 정리 · 요약, 내부 보고 및 준법 관련 문서 작성 지원 • **준법 리스크 모니터링:** 고객 응대 기록, 내부 커뮤니케이션, 운용 보고서 분석 기반 잠재적 준법 리스크 및 이상 징후 탐지

자료: 삼일PwC경영연구원

2.3 자산운용업의 AI 확산에 따른 새로운 과제의 부상

AI 활용이 실제 업무 흐름과 정보 처리 구조에 내재화되면서 기존 내부통제 체계 간 괴리 확대

자산운용업에서 AI 활용이 새로운 관리 이슈로 연결되는 핵심 배경은 AI가 실제 업무 운영 과정과 정보 흐름 구조 전반에 영향을 미치기 시작했다는 점에 있다. 과거 자산운용업의 업무 환경은 내부 시스템과 정형 데이터 중심의 비교적 폐쇄적인 구조 아래 운영되어 왔으며, 업무 수행과 승인 절차 역시 사전에 정의된 프로세스를 기반으로 이루어지는 경우가 많았다. 이에 따라 누가 어떠한 정보를 바탕으로 판단했고, 어떠한 절차를 거쳐 검토 · 승인했는지, 최종 책임이 누구에게 있는지를 비교적 명확하게 구분할 수 있었다.

그러나 최근에는 생성형 AI와 외부 AI 서비스, SaaS 기반 도구, 응용 프로그램 프로그래밍 인터페이스(Application Programming Interface, API) 연계 기능 등이 실제 업무 과정 안으로 빠르게 결합되면서, 과거 내부 시스템 중심으로 운영되던 자산운용업의 업무 환경 역시 빠르게 변화하고 있다. 특히 비정형 데이터와 외부 데이터 활용, 자동화 워크플로우(Workflow) 기반 업무 처리 등이 확대되면서 업무 방식과 정보 흐름 구조 역시 이전보다 훨씬 복잡해지고 있다.

변화하는 AI 활용 환경과 외부 서비스 연계 확산에 따른 지속가능한 통제·관리 체계 구축 필요성 증대

이러한 변화는 기존 내부통제 체계가 전제해 온 운영 환경과 실제 업무 구조 사이의 괴리를 점차 확대시키고 있다. 과거 내부통제 체계는 비교적 정형화된 승인 절차와 시스템 중심 통제 환경을 기반으로 운영되어 왔으나, 최근에는 외부 AI 서비스와 자동화 기능 등이 실제 업무 흐름 안으로 빠르게 연결되면서 기존 방식만으로는 변화하는 업무 환경을 충분히 관리하기 어려워질 가능성이 커지고 있다.

예를 들어 과거에는 내부 시스템 안에서 제한된 데이터와 업무 절차를 중심으로 통제가 이루어졌다면, 최근에는 외부 생성형 AI 서비스와 API 연계 기능 등을 활용해 현업 부서가 실시간으로 다양한 정보와 기능을 활용하는 환경이 확대되고 있다. 이에 따라 기존의 사후 점검 중심 통제 방식만으로는 실제 운영 현황과 데이터 흐름, 외부 서비스 활용 구조 등을 지속적으로 파악 · 관리하기 어려운 측면 역시 존재한다.

또한 생성형 AI 환경에서는 모델 업데이트와 활용 환경 변화에 따라 결과와 기능 구조가 지속적으로 달라질 가능성이 존재하며, 실제 업무 과정 안에서도 새로운 기능과 자동화 흐름이 반복적으로 추가 · 변경될 수 있다. 이처럼 AI 활용 구조 자체가 계속 변화하는 환경에서는 기존과 같은 고정형 통제 체계만으로 운영 안정성을 유지하기 어려워질 가능성 역시 커지고 있다.

이와 함께 자산운용업은 고객 자산과 투자 판단, 시장 신뢰가 직접 연결되는 산업이라는 점에서, AI 활용 과정에서 발생할 수 있는 오류나 통제 실패는 투자자 보호와 시장 신뢰 훼손 문제로 이어질 가능성 역시 존재한다. 특히 실제 투자 판단과 리스크 관리, 고객 관련 업무 과정 안에서 AI 활용 범위가 확대될수록, AI 결과물과 데이터 활용 과정이 적절한 기준 아래 운영되고 있는지를 지속적으로 관리해야 할 필요성 역시 함께 커지고 있다.

그 결과 자산운용업 내 AI 활용 확대는 변화하는 업무 운영 구조와 데이터 흐름, 외부 서비스 연계 환경 등을 내부통제 체계 안에서 어떻게 안정적으로 관리할 것인가의 문제로 연결된다. 이에 따라 최근 자산운용업의 AI 논의는 AI 활용 범위와 허용 기준, 데이터 관리 방식, 외부 AI 서비스 활용, 접근 권한과 기록 관리, 내부통제 및 책임 구조 등을 어떠한 기준 아래 운영 · 관리할 것인가의 방향으로 빠르게 확장되고 있다.

AI 확산에 따른 자산운용업의 통제 방식 변화

구분	기존 자산운용업 통제 체계	AI 활용 확대 이후 변화
업무 수행 방식 변화	• 사전 정의된 업무 프로세스와 승인 절차를 기반으로 정형화된 업무 수행 • 인간 중심의 투자 분석 및 의사결정 수행 • 업무 보조 수준의 제한적 자동화	• 현업 부서가 생성형 AI와 외부 AI 서비스를 활용해 실시간 분석 · 문서 생성 · 자동화 기능을 직접 활용하는 환경 확대 • AI 기반 분석, 추천, 리서치 보조 등의 기능이 투자 판단 과정 전반에 영향을 미치는 구조로 변화 • AI 에이전트 기반 업무 자동화 확대와 함께 이메일 발송, 데이터 조회, 보고서 작성, API 호출 등 실제 업무 수행 영역으로 확장
데이터 및 시스템 통제 구조 변화	• 내부 시스템 및 정형 데이터 중심의 폐쇄형 운영 환경 • 내부 데이터 중심의 제한적 정보 활용 구조 • 시스템별로 분리된 개별 운영 구조	• 외부 데이터, 생성형 AI, API, 클라우드 서비스 등이 연결되는 개방형 · 연계형 업무 환경 확대 • 비정형 데이터, 자연어 기반 정보, 외부 데이터 · 오픈소스 활용 증가 • 내부 데이터 중심의 폐쇄형 운영 환경에서 외부 AI 서비스 연계 기반 업무 환경으로 변화
통제 및 거버넌스 방식 변화	• 규칙 기반(Rule-based)의 사전 정의형 통제 체계 중심 운영 • IT · 보안 부서 중심의 기술 통제 구조 • 사후 점검 중심의 내부통제 체계 • 명확한 승인 절차와 책임 경계를 전제로 한 업무 구조	• 실시간 활용 · 비정형 업무 확대에 따라 운영 과정 중심의 지속적 통제 필요성 확대 및 현업 · 준법 · 보안 부서가 함께 참여하는 운영 중심 AI 거버넌스 중요성 확대 • AI · 현업 부서 · 외부 사업자 간 역할과 책임 구조가 상호 연결되면서, 승인 · 책임 체계 복잡성 확대 • AI 활용 현황과 접근 권한, 로그 기록, 업무 흐름 등을 지속적으로 식별 · 관리해야 하는 운영 구조로 변화
보안 및 리스크 환경 변화	• 내부 시스템 안정성과 접근 권한 관리 중심의 보안 체계 • 내부 시스템 장애 · 전통적 IT 리스크 중심 관리 • 시스템 결과값에 대한 정형화된 검증 구조	• 프롬프트 인젝션, 권한 오남용, AI 결과물 왜곡 등 AI 관련 보안 이슈 부상 • 외부 AI 서비스, 클라우드, API, 오픈소스 등에 대한 공급망 · 제3자 리스크 확대 • AI 결과물에 대한 검증 가능성 · 책임 추적성 및 감사 체계 중요성 확대
내부통제 목적 변화	• 내부 운영 안정성과 규정 준수 중심의 내부통제 • 정형화된 업무 절차와 사후 점검 중심 관리 • 시스템 및 조직 단위 중심 통제 구조	• AI 활용 확대 과정에서도 투자자 보호, 책임성, 내부통제의 신뢰성을 실제 운영 과정 안에서 유지해야 하는 방향으로 확대 • 인간 검토 · 승인 체계 대신 실시간으로 관리 · 통제의 필요성 증대 • 데이터 · AI · 외부 서비스 · 현업 조직이 연결된 운영 환경 전반을 관리하는 거버넌스 체계 중요성 확대

자료: 삼일PwC경영연구원

03

AI 확산에 따른 자산운용업의 새로운 거버넌스 이슈

3.1 현업 중심 AI 확산과 관리 범위 밖 AI 활용 확대

자산운용업계 내 AI 활용 효율성이 우선 강조되며 내부통제 기준 정비보다 현업의 AI 활용이 먼저 확산되는 양상

국내 자산운용업에서 AI 활용이 빠르게 확대되면서, 기존 준법 · 내부통제 체계와 실제 현업의 AI 활용 방식 간 괴리가 점차 확대되고 있다. 최근에는 클로드(Claude), 챗GPT(ChatGPT), 제미나이(Gemini) 등 범용 생성형 AI 서비스와 SaaS 기반 도구 활용이 확산되면서, 리서치 자료 작성과 투자 아이디어 검토, 데이터 분석 지원, 보고서 작성 등 다양한 업무 영역에서 AI 활용이 빠르게 증가하고 있다. 문제는 이러한 AI 활용이 조직 차원의 통합된 준법 · 내부통제 체계 안에서 관리되기보다, 현업 조직의 실무 수요와 업무 효율성 중심으로 먼저 확산되는 경우가 많다는 점이다.

자산운용업은 정보의 해석과 판단 자체가 실제 투자 의사결정과 운용 성과로 직접 연결되는 산업이라는 점에서, AI 활용의 영향이 다른 금융업권보다 더욱 직접적으로 나타나는 특성을 가진다. 특히 시장 대응 속도와 운용 성과 압박이 강하게 작동하는 국내 자산운용업 환경에서는 현업 조직이 업무 효율성과 정보 처리 속도 향상을 위해 AI 활용을 우선 확대하려는 유인이 크다. 반면 준법감시 · 리스크 관리 · 정보보호 등 백오피스 조직은 상대적으로 사후적 통제 기능으로 인식되는 경우가 많아, 실제 현업의 AI 활용 속도가 조직 차원의 준법 · 내부통제 체계 정비 속도를 앞지르는 상황이 나타나고 있다.

자산운용업의 AI 확산 관련 내부통제 관리 한계가 나타나는 주요 원인

성과 · 수익 중심의 프론트 조직 문화 투자 성과와 수익 창출이 핵심 경쟁력으로 작동하는 산업 특성상, 업무 효율성과 투자 속도가 내부통제 절차보다 우선시되는 경향 강화	**정보 해석 · 판단 중심 산업 구조** 시장 · 기업 · 산업 정보를 빠르게 해석하고 투자 판단으로 연결해야 하는 특성상 생성형 AI 활용 수요 확대	**투자 판단 과정과 AI 활용 간 경계 모호화** AI가 리서치 · 시장 분석 · 투자 아이디어 검토 등 실제 투자 판단 과정에 영향을 미치면서 책임과 승인 경계가 불명확해지는 구조 심화	**비정형 정보 활용 비중이 높은 업무 특성** 뉴스 · 공시 · 컨퍼런스콜 · 리서치 자료 · 대체 데이터 등 비정형 정보 활용 비중이 높다는 점에서 생성형 AI 활용 확대 유인이 높음
통제 밖 AI 활용 확대 가능성 운용역과 리서치 조직이 업무 효율화를 위해 외부 AI 서비스를 직접 활용하면서 중앙 통제 체계 밖 활용 증가 가능성	**제한적 백오피스 · 통제 조직 운영** 일부 중소형 운용사와 사모펀드 운용사의 경우, 수익 창출 조직 중심 운영으로 인해 준법 · 보안 · 내부통제 기능이 상대적으로 제한되는 구조	**시장 대응 속도 중심 업무 환경** 시장 변화에 대한 신속한 대응이 중요한 산업 특성상, AI 기반 정보 분석 · 자동화 활용 압력이 다른 금융권 대비 강하게 작동	**AI 활용 대비 거버넌스 · 규제 이해 부족** 생성형 AI 활용은 빠르게 확산되는 반면, 책임 구조와 데이터 관리, 보안 · 기록 통제 등 AI 거버넌스 운영 경험은 아직 충분히 축적되지 않은 상황

자료: 삼일PwC경영연구원

현업 중심 AI 활용 확산은 조직 차원의 통제 체계 안으로 편입해야 하는 과제로 확장

특히 기존 내부통제 체계가 승인된 시스템과 정형화된 업무 프로세스, 명확한 권한 구조를 전제로 설계되어 온 반면, 생성형 AI의 경우, 현업 부서가 외부 서비스와 API를 직접 연결 · 조합해 다양한 업무 자동화 구조를 빠르게 구축할 수 있다는 점에서 기존 내부통제 체계가 전제해 온 운영 방식과 구조적으로 충돌하는 양상이 나타나고 있다.

실제로 현업 부서가 별도의 시스템 구축 없이 외부 AI 서비스와 생성형 AI API를 활용해 리서치 요약, 투자정보 정리, 보고서 작성, 이메일 생성, 데이터 조회 등의 기능을 자동화하는 사례 역시 빠르게 증가하고 있다. 나아가 현업 부서를 중심으로 다양한 자동화 기능과 업무 흐름이 개별적으로 구축되면서, 조직 차원에서는 실제 어떤 AI 서비스와 자동화 기능이 어떤 업무에 활용되고 있는지를 통합적으로 파악 · 관리하기 어려워질 수 있다.

이에 따라 입력 정보와 결과 활용 범위, 외부 서비스 활용 현황 등에 대한 지속적인 관리 · 통제 역시 어려워질 수 있으며, 승인되지 않은 AI 활용과 섀도우 AI(조직의 공식 승인이나 관리 범위 밖에서 생성형 AI가 활용되는 현상을 의미, Shadow AI) 형태의 운영 역시 점차 확산될 수 있다. 이는 일부 업무가 조직의 공식 관리 체계 밖에서 운영되는 AI 기반 자동화 구조로 전환될 수 있다는 점에서 보다 구조적인 운영 리스크로 이어질 수 있다. 특히 현업 부서가 외부 AI 서비스와 자동화 기능을 직접 활용하는 과정에서 기존 내부통제 체계가 전제한 승인 절차와 권한 구조, 검증 체계가 우회되거나 충분히 적용되지 못할 가능성이 존재한다.

데이터 수집과 정보 요약, 분석 및 투자 시그널 생성 과정 등이 AI 기반 자동화 구조로 연결되면서, 업무 효율성과 속도를 우선하는 자동화 운영 방식이 조직 차원의 검증 및 관리 체계보다 먼저 정착될 가능성도 커지고 있다. 이 과정에서 외부 AI 모델의 응답 오류와 현업 부서의 자동화 로직 문제 등이 복합적으로 발생할 경우 실제 업무 운영 과정의 복잡성과 책임 문제 역시 더욱 확대될 수 있다. 특히 중소형 자산운용사의 경우 제한된 인력과 비용 구조로 인해 AI 활용 현황을 전사적으로 관리 · 통제할 수 있는 운영 체계 구축에 어려움을 겪을 가능성이 크다.

이와 같이 현업 중심의 자동화와 비공식 AI 활용이 확대되는 환경에서는 조직 차원에서 실제 AI 활용 현황과 운영 리스크를 충분히 파악·관리하기 어려워질 수 있다. 이에 따라 자산운용업에서는 현업 중심의 AI 활용과 비공식 자동화 구조를 조직 차원에서 어떻게 식별 · 관리할 것인가가 중요한 운영 과제로 부상하고 있다.

3.2 AI 기반 데이터 활용 다변화와 정보 흐름 복잡화

데이터 거버넌스는 AI 환경에서 투자자 보호와 내부통제 신뢰성을 뒷받침하는 핵심

자산운용사는 시장 데이터와 기업 공시, 뉴스, 고객정보, 거래정보, 대안 데이터 등 다양한 정보를 활용하고 있으며, 최근에는 비정형 데이터와 외부 데이터 활용 역시 확대되는 추세이다. 이에 따라 데이터의 품질과 출처, 적법성뿐 아니라 데이터가 어떠한 경로로 수집·가공·활용되고 있는지를 체계적으로 관리할 필요성도 함께 높아지고 있다.

AI 환경에서 데이터 관리는 AI 결과물의 신뢰성과 내부통제 수준을 결정하는 핵심 요소로 자리잡고 있으며, 데이터 활용 전 과정에 대한 체계적인 거버넌스 구축의 중요성도 더욱 커지고 있다. 무엇보다도 데이터 관리 이슈는 AI 활용 과정 전반에 대한 통제 가능성과 책임 체계를 확보하기 위한 핵심 기반으로 작용하기 때문이다.

AI 기반 업무 환경은 데이터 흐름 중심 통제 체계 중요성을 확대

개인정보 및 비공개정보 활용 문제는 가장 직접적인 규제 및 내부통제 리스크 중 하나이다. 자산운용사는 투자자 성향 분석과 고객 맞춤형 서비스, 리서치 자동화, 내부 리스크 관리 등 다양한 영역에서 고객정보와 거래 데이터를 활용할 가능성이 있으며, 이 과정에서 개인정보와 거래 데이터의 활용 범위, 저장 방식, 외부 활용 가능 범위 등을 보다 세밀하게 관리해야 할 필요성 역시 커지고 있다.

특히 생성형 AI 환경에서는 고객정보와 내부 데이터가 다양한 AI 분석 과정과 외부 서비스 안에서 이동 · 결합될 가능성이 커지면서, 데이터 흐름 자체를 일관되게 추적 · 관리해야 할 필요성 역시 확대되고 있다. 또한 투자 관련 내부자료와 미공개 정보, 운용전략 정보 등이 AI 분석 과정에 활용될 경우, 정보관리 통제와 이해상충 관리 측면에서도 추가적인 관리 부담이 발생할 수 있다.

데이터 품질과 출처 문제 역시 핵심 관리 이슈로 부상하고 있다. AI 모델은 학습에 활용된 데이터의 품질과 편향을 그대로 반영하는 특성이 있으며, 데이터 자체가 부정확하거나 특정 시장 환경에 편중되어 있을 경우 결과 역시 왜곡될 수 있다. 특히 AI 기반 분석은 인터넷 기반 공개 데이터와 다양한 외부 정보를 광범위하게 활용한다는 점에서, 데이터의 사실 정확성과 최신성을 충분히 검증하지 않을 경우 결과 왜곡 가능성 역시 함께 커질 수 있다. 따라서 이는 AI 기반 투자 분석과 의사결정 전반의 신뢰성과 연결되는 이슈로 볼 수 있다.

또한 최근에는 데이터 활용 범위와 정보 흐름 자체가 빠르게 복잡해지면서, 데이터 이동 구조와 활용 기준을 일관되게 파악하기 어려워지는 사례 역시 증가하고 있다. 과거에는 정형화된 내부 데이터 중심의 분석이 주를 이루었다면, 최근에는 다양한 외부 정보와 비정형 데이터를 결합한 AI 기반 분석 활용이 확대되면서 데이터 출처와 활용 범위, 데이터 간 결합 방식 등에 대한 보다 정교한 통제가 요구되고 있다. 특히 AI 분석 과정에서는 어떠한 데이터가 어떤 경로를 거쳐 활용되었는지를 지속적으로 확인할 수 있는 데이터 추적 가능성(Traceability) 확보에 대한 요구 역시 강화되고 있다.

이러한 변화는 AI 환경에서 데이터의 출처와 이동 흐름, 활용 기준에 대한 관리 범위가 빠르게 확대되고 있음을 보여준다. 이에 따라 데이터의 출처와 적법성, 품질 검증 절차, 민감정보 처리 기준, 데이터 활용 기준, 접근 권한과 로그관리 체계 등에 대한 관리 중요성 역시 함께 확대되고 있다. 특히 AI 환경에서는 데이터 활용과 이동 흐름이 어떻게 이루어지고 있는지에 대한 지속적인 파악과 검증이 운영 안정성 확보의 전제조건으로 자리 잡고 있다.

AI 환경에서의 데이터 흐름 구조도 및 관리 범위 확대

자료: 삼일PwC경영연구원

3.3 다층적 규제 환경과 AI 운영관리 부담 확대

금융권의 AI 활용은 AI 기본법뿐 아니라, 개인정보보호법 · 신용정보법 등 여러 규제가 동시에 적용되는 다층적 규제 영역

자산운용업의 AI 활용 확대에 따라 AI 활용 과정 전반을 조직 차원에서 어떠한 기준과 체계 아래 관리할 것인가의 문제가 중요한 과제로 부상하고 있다. 특히 생성형 AI 활용이 업무 프로세스 전반으로 확산되면서, AI 활용 과정 역시 기존 준법 · 내부통제 · 정보보호 체계 전반과 직접적으로 연결되기 시작하고 있다. 이에 따라 AI 활용은 기존 내부통제와 준법, 정보보호 체계 전반을 동시에 고려해야 하는 복합 관리 영역으로 변화하고 있다.

특히 금융권의 AI 활용은 AI 기본법 단독으로 규율되는 구조가 아니라, 개인정보보호법과 신용정보법, 전자금융거래법, 금융보안 규정, 업무위탁 및 클라우드 규제, 내부통제 기준 등 여러 규제 체계가 동시에 적용되는 다층적 규제 영역에 해당한다. 이에 따라 금융권의 AI 활용은 일반 산업 대비 훨씬 복합적인 운영 · 준법 이슈와 관리 부담을 수반하게 된다.

특히 AI 기반 투자 분석과 고객 정보 활용 과정에서는 데이터 보관과 접근 권한 관리, 기록 보존, 외부 서비스 승인, 정보보호 기준 등 다양한 내부통제 요소가 동시에 연결될 수 있다. 문제는 실제 현업 부서 단위에서 이러한 다층적 규제와 내부통제 요구사항을 개별적으로 충분히 검토 · 이행하기 어렵다는 점이다.

AI 활용은 조직 차원의 관리 기준과 운영 체계 아래 지속적으로 관리 · 운영해야 하는 핵심 관리 이슈

최근 AI 활용이 확대되면서 다양한 AI 기능과 자동화 구조가 실제 업무 과정 안으로 빠르게 연결되고 있다. 그러나 실제 AI 활용 과정에서는 입력 가능한 정보 범위와 비공개정보 활용 여부, 외부 서비스 승인, 데이터 저장 위치, 접근 권한 관리, 기록 보존, 결과 활용 범위 등 다양한 관리 요소들이 동시에 연결될 수 있으며, 이러한 요소들은 개별 현업 조직 차원에서 단독으로 판단 · 관리하기 어려운 성격을 가진다.

더불어 AI 활용 구조는 기능과 활용 범위가 지속적으로 변화하는 특성으로 인해 기존의 관리 방식만으로는 대응하기 어려운 측면이 존재한다. 특히 생성형 AI 환경에서는 실제 업무 과정 안에서 다양한 기능과 자동화 흐름이 수시로 추가 · 변경될 수 있다는 점에서 기존 시스템 중심 통제 방식만으로는 실제 운영 현황을 충분히 관리하기 어려울 가능성이 존재한다.

과거에는 신규 시스템 도입 시 사전 승인과 구축 단계 중심으로 통제가 이루어지는 경우가 많았지만, 생성형 AI와 SaaS 기반 AI 서비스는 현업 조직이 다양한 기능과 워크플로우를 지속적으로 추가 · 변경하며 활용할 가능성이 높다. 이에 따라 기존 업무 프로세스 일부 역시 지속적으로 변화 · 재구성되고 있으며, AI 활용 과정 전반을 상시적으로 모니터링하고 관리할 수 있는 운영 체계의 중요성 역시 더욱 커지고 있다.

이러한 점에서 자산운용업의 AI 활용은 개별 현업 조직 단위의 효율화 문제에 머물지 않고, 조직 차원의 관리 기준과 운영 체계 아래 지속적으로 관리해야 하는 핵심 관리 이슈로 전환되고 있다. 특히 AI 활용 범위와 허용 기준, 데이터 활용 정책, 외부 AI 서비스 승인, 위험관리 기준, 기록 관리 체계, 역할과 책임 구조 등을 조직 차원의 일관된 기준 아래 지속적으로 관리 · 운영할 수 있는 체계의 중요성이 더욱 커지고 있다.

이에 따라 자산운용업의 AI 관련 핵심 과제는 다층적 규제 환경과 내부통제 요구사항에 대응할 수 있도록, AI 활용 과정 전반을 조직 차원에서 지속적으로 관리 · 운영할 수 있는 체계를 어떻게 정비할 것인가의 문제로 확대되고 있다.

자산운용업 내 AI 활용 확대와 데이터·운영 관리 체계 변화

AI 활용 범위 및 업무 적용 확대

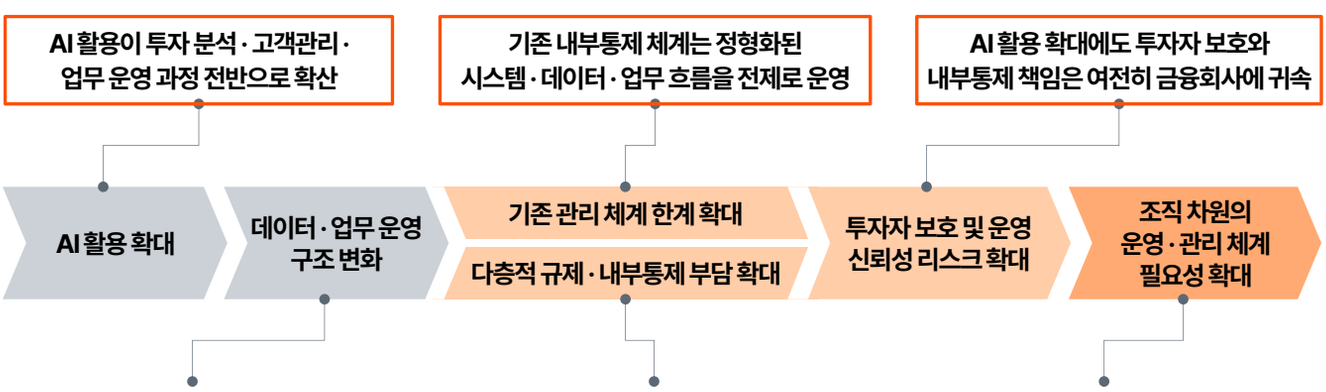
- 생성형 · 에이전틱 AI 기반 업무 활용 확대
- AI 기반 투자 분석 및 고객 정보 활용 확대
- 업무 자동화 및 AI Workflow 활용 증가
- 외부 AI · SaaS 기반 업무 지원 환경 확산
- 비정형 데이터 기반 분석 활용 확대
- 현업 중심 AI 활용 범위 전반 확대

기존 내부통제 · 데이터 관리 체계 한계 확대

- 데이터 활용 과정 추적 어려움 확대
- 기존 승인 · 기록 관리 체계 한계 노출
- 데이터 출처 · 활용 범위 관리 부담 증가
- 접근 권한 · 기록보존 · 정보보호 관리 복잡성 확대
- 비정형 · 실시간 데이터 흐름 증가
- 기존 시스템 중심 통제 방식 실효성 저하 가능성

AI 환경에서 데이터 · 의사결정 신뢰성 리스크 확대

- 투자 판단과 데이터 품질 간 연결성 확대
- AI 결과 왜곡 및 오류 가능성 확대
- 내부자료 · 미공개정보 활용 리스크 확대
- 정보관리 통제 및 이해상충 관리 부담 증가
- 운영 안정성 및 감사 대응 중요성 확대
- 설명 · 검증 · 추적 가능성 중요성 확대



AI 기반 데이터 흐름 · 운영 구조 복잡화

- 데이터 흐름 및 정보 연계 구조 복잡화
- 외부 AI · API · 클라우드 연계 확대
- 실시간 분석 · 업무 처리 환경 확산
- 데이터 이동 · 결합 구조 복잡성 확대
- 다양한 외부 정보 · 비정형 데이터 활용 확대
- AI 중심 업무 흐름 및 운영 환경 형성

AI 활용 과정과 규제 · 내부통제 요구사항 간 연결 확대

- 개인정보 · 신용정보 · 전자금융 · 금융보안 규제 동시 적용
- 업무위탁 · 클라우드 · 내부통제 기준 동시 연계
- 데이터 보관 · 접근 권한 · 기록보존 요구 확대
- 외부 AI 서비스 승인 및 관리 부담 확대
- 현업 조직 단위의 단독 검토 · 이행 한계 확대
- AI 활용 과정 전반에 대한 상시 관리 필요성 확대

AI 활용 전반에 대한 조직 차원의 지속 관리 필요성 확대

- AI 활용 범위 및 허용 기준 정립
- 데이터 활용 정책 및 승인 기준 수립
- 외부 AI 서비스 및 위험관리 기준 정비
- 기록 관리 및 데이터 흐름 추적 체계 구축
- 현업 · 준법 · IT · 보안 조직 간 협업 중요성 확대
- AI 활용 과정 전반에 대한 지속적 모니터링 필요

기존 정형화된 내부 데이터 중심 구조에서 데이터 · 외부 AI · 자동화 흐름이 연결되는 운영 구조로 변화

AI 활용은 다층적 규제와 내부통제 요구사항이 동시에 적용되는 복합 관리 영역으로 변화

AI 활용 과정 전반을 조직 차원의 관리 기준과 운영 체계 아래 지속적으로 관리할 수 있는 체계 구축이 핵심 과제로 부상

자료: 삼일PwC경영연구원

[Appendix] 국내 금융권 AI 규제 환경과 주요 고려사항

국내 금융권의 AI 규제 환경은 단일 법률이나 특정 감독 기준만으로 설명하기 어려운 다층적 구조를 형성하고 있다. 최근 금융회사들의 AI 활용이 빠르게 확대되면서, 개인정보 보호와 자동화된 의사결정, 정보보호, 업무위탁, 설명 가능성, 내부통제 등 기존 금융 · 데이터 · 보안 규제 체계 위에 AI 관련 규제가 추가적으로 중첩되는 형태가 나타나고 있다. 이에 따라 금융회사들은 하나의 AI 활용 행위가 어떠한 규제와 내부통제 요구사항에 동시에 연결되는지를 함께 검토해야 하는 환경에 놓이게 되었다.

최근 가장 큰 변화 중 하나는 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법(AI 기본법)」의 시행이다. AI 기본법은 2024년 12월 국회를 통과했으며, 2026년 1월 시행 이후 현재 하위법령과 세부 가이드라인 정비가 진행되고 있다. 해당 법은 국내 최초의 AI 일반법 성격을 가지며, 고영향 AI와 생성형 AI에 대한 안전성 · 신뢰성 · 투명성 확보 의무 등을 규정하고 있다.

특히 금융권에서는 여신심사와 투자 판단, 고객 평가, 추천 서비스 등 개인의 권리 · 의무 관계에 영향을 미치는 영역에서 AI 활용이 확대되고 있다는 점에서, 일부 영역은 향후 '고영향 AI'로 분류될 가능성 역시 존재한다. 이에 따라 금융회사는 AI 활용 과정에서 AI 기본법상 의무사항과 감독 기준을 함께 검토해야 하는 환경에 놓이게 되었다. 더불어 현재 과학기술정보통신부를 중심으로 고영향 AI 판단 기준과 AI 영향평가 관련 세부 기준 논의가 진행되고 있다는 점에서, 향후 금융권 AI 활용에 대한 감독과 관리 요구 역시 보다 구체화될 가능성이 높다.

국내 금융권의 실제 AI 활용 과정에서는 AI 기본법뿐만 아니라, 개인정보보호법과 신용정보법, 전자금융거래법, 금융소비자보호법, 전자금융감독규정, 업무위탁 규정 등 기존 금융 · 데이터 · 보안 규제 체계 역시 동시에 적용된다. 특히 AI 활용 과정에서 고객 정보나 개인신용정보가 사용되는 경우에는 개인정보 처리와 자동화된 의사결정 관련 규제까지 함께 고려해야 한다.

예를 들어 개인정보보호법과 신용정보법은 자동화된 의사결정에 대한 설명 요구 및 이의제기 관련 권리 등을 규정하고 있다. 이에 따라 금융회사가 AI 기반 분석과 추천, 평가 시스템을 활용하는 경우에는 설명 가능성과 기록 관리 체계 역시 함께 요구될 수 있다.

외부 생성형 AI 서비스 및 클라우드 · SaaS 기반 AI 도구 활용 확대 역시 금융권의 규제 대응 복잡성을 높이는 요인으로 작용하고 있다. 최근 금융권에서는 생성형 AI를 활용한 문서 작성과 리서치 지원, 데이터 분석 등이 빠르게 확대되고 있으나, 이러한 활용은 동시에 정보 유출과 외부 서비스 통제, 업무위탁, 정보처리 위탁 문제와 연결될 수 있다. 특히 금융회사가 외부 AI 서비스를 활용하는 경우, 해당 활용 방식이 보조적 업무 도구 목적인지, 업무위탁에 해당하는지, 또는 정보처리 위탁 규제 적용 대상인지에 대한 검토 역시 필요하다. 이는 금융회사의 AI 활용이 정보보호와 업무위탁, 외부 서비스 통제 등 복수의 규제 이슈와 동시에 연결될 수 있음을 보여준다.

한편 금융당국은 AI 기본법 이전부터 금융권 AI 활용과 관련한 별도 가이드라인 체계를 운영해 왔다. 대표적으로 「금융분야 AI 운영 가이드라인」(2021), 「금융분야 AI 개발 · 활용 안내서」(2022), 「금융분야 AI 보안 가이드라인」(2023) 등을 통해 금융권 AI 활용 기준을 지속적으로 정비하고 있다. 이러한 가이드라인은 법적 강제 규정은 아니지만, 실제 금융회사 내부통제 및 감독 대응 과정에서는 사실상 중요한 관리 기준으로 작동하고 있다. 특히 금융당국은 최근 생성형 AI 활용 확대에 대응해 금융권의 AI 활용 활성화와 함께 책임 있는 AI 활용 체계 구축 필요성을 지속적으로 강조하고 있다.

문제는 이러한 규제 구조가 기능별 · 영역별로 분산되어 있다는 점이다. 특히 생성형 AI나 자율 기반 AI 서비스처럼 활용 방식 자체가 빠르게 변화하는 환경에서는, 금융회사 입장에서 하나의 AI 활용 행위가 어떠한 규제와 내부통제 요구사항에 해당하는지를 지속적으로 판단해야 하는 부담 역시 커지고 있다. 이에 따라 금융회사들은 AI 활용 전반을 기존 내부통제와 규제 체계 안에서 어떻게 관리 가능한 영역으로 편입시킬 것인가에 대한 통합적 대응 체계를 함께 구축할 필요성이 커지고 있다.

국내 금융권 AI 활용 관련 주요 규제 · 가이드라인

국내 규제 · 가이드라인	핵심 설명
인공지능기본법 고영향 AI, 생성형 AI 고지 · 표시, 투명성, 안전성 확보 등	• 2026년 1월 22일부터 시행된 AI 일반법으로, 생성형 · 고영향 AI를 이용자에게 제공하는 경우 AI 기반 운용 사실 고지 등 투명성 확보 의무가 핵심 • 금융 분야에서는 신용평가 · 대출심사 등 일부 영역이 고영향 AI와 연결될 수 있으나, 모든 금융 AI가 일괄적으로 고영향 AI에 해당하는 것은 아니므로 구체적 용도별 판단 필요
개인정보보호법 개인정보 처리, 가명정보, 자동화된 결정, 정보주체 권리 등	• AI가 개인정보를 처리하거나 자동화된 결정을 수행하는 경우 처리 근거, 목적 제한, 최소 수집, 안전조치가 핵심 쟁점 • 자동화된 결정에 대해서는 거부 · 설명 · 검토 요구 등 정보주체 권리 대응 체계 필요
신용정보법 개인신용정보, 자동화평가, 프로파일링 대응권 등	• AI가 개인신용평가, 금융거래 설정 · 유지 여부 판단 등 개인신용정보 기반 자동화평가에 활용되는 경우 설명 요구, 기초정보 정정 · 삭제, 재산출 요구 대응 필요 • 단, 일반적인 업무 효율화 AI보다는 신용정보 기반 평가 · 판단 업무와 연결될 때 직접성이 커짐
금융분야 AI 가이드라인 등 합법성, 신뢰성, 보안성 등 AI 거버넌스	• 금융권 AI 활용의 감독상 기준으로, 2025년 공개된 통합 가이드라인(안)은 거버넌스, 합법성, 보조수단성, 신뢰성, 금융안정성, 신의성실, 보안성을 7대 원칙으로 제시 • 법령상 직접 의무라기보다 모범규준 · 업권별 자율규제 형식으로 운영될 예정이라는 점을 구분할 필요
금융분야 AI 보안 가이드라인 AI 모델 보안, 학습데이터 관리, API 보안, 챗봇 보안 등	• 금융보안원이 제시한 AI 보안 기준으로, AI 모델 개발 단계별 보안사항과 AI 챗봇 보안 체크리스트를 포함 • API 키 관리, 이상행위 모니터링, 모델 · 데이터 보안 등 AI 특화 보안 점검에 활용 가능
전자금융거래법·전자금융감독규정 접근통제, 로그관리, 망분리, 클라우드 · SaaS, 사고 대응 등	• AI가 내부 시스템, 전자금융 인프라, API, 클라우드 · SaaS와 연결될 경우 접근 권한, 로그, 이상행위 모니터링, 장애 · 침해사고 대응 체계와 연결 • 특히 2026년 4월부터 내부 업무망 SaaS 활용 예외가 일정한 보안규율 준수를 전제로 허용되는 방향으로 개선
금융소비자보호법 적합성 · 적정성, 설명의무, 부당권유 금지, 광고 규제 등	• AI가 고객 응대, 금융상품 추천, 투자성향 분석, 마케팅 문안 작성에 활용될 경우 기존 금융상품 판매규제와 연결 • AI가 만든 산출물이라도 설명의무, 적합성 원칙, 부당권유 금지 등 금융소비자보호 체계 안에서 관리 필요
자본시장법 투자권유, 설명의무, 불공정거래, 미공개 중요정보 관리 등	• 자산운용사 · 금융투자업자가 AI를 리서치, 투자 판단 지원, 고객 설명, 투자권유 자료 작성에 활용하는 경우 자본시장법상 투자자 보호 규제와 연결 • 특히 미공개 중요정보 관리, 불공정거래 방지, 투자권유 및 설명자료 검토 체계가 AI 활용 과정에서도 유지되어야 함

자료: 국가법령정보센터, 금융위원회, 금융감독원, 개인정보보호위원회, 금융보안원 자료 종합, 삼일PwC경영연구원 재구성

3.4 생성형 AI 환경에서의 보안 · 권한 관리 리스크 확대

AI 활용 확대는 정보 유출 및 비인가 접근 등 새로운 보안 이슈를 유발

최근 금융산업에서는 생성형 AI가 투자정보 분석과 내부 지식 검색, 업무 자동화 등 핵심 업무 영역 안으로 빠르게 확산되면서 새로운 형태의 보안 리스크 역시 함께 확대되고 있다. 특히 생성형 AI는 외부 서비스와 다양한 업무 시스템에 손쉽게 연결될 수 있다는 점에서, 기존 금융회사가 전제해 온 보안 통제 체계만으로는 충분히 대응하기 어려운 새로운 운영 환경을 만들어내고 있다.

가장 직접적인 우려는 내부정보 유출 가능성이다. 생성형 AI는 사용자가 입력한 데이터를 기반으로 응답을 생성하는 구조이기 때문에, 업무 효율화를 목적으로 고객정보, 투자 전략, 미공개 리서치 자료, 내부 회의자료, 소스코드 등을 외부 AI 서비스에 입력할 경우 민감정보 유출 문제가 발생할 수 있다. 특히 생성형 AI는 입력된 정보가 외부 시스템 안에서 처리 · 활용되는 구조라는 점에서, 정보 이동과 활용 범위를 기존 방식처럼 직접 통제하기 어려운 특성을 가진다. 이는 개인정보보호법, 신용정보법, 전자금융 관련 규제, 계약상 비밀유지 의무 등과 연결되며, 금융회사 입장에서는 규제 · 운영 · 평판 리스크가 동시에 발생할 수 있는 문제로 이어진다.

비공식 AI 활용에 따른 정보 유출 리스크 역시 금융회사에서 중요한 이슈로 부상하고 있다. 생성형 AI는 접근성과 활용 편의성이 매우 높다는 점에서, 조직 차원의 관리 범위 밖에서 활용될 가능성이 존재한다.

프롬프트 인젝션 관련 주요 내용

구분	핵심 내용	상세 및 시사점
공격 경로	• 외부 공격자뿐 아니라 내부 사용자도 공격 주체가 될 수 있음 • 채팅 입력, 문서, 이메일, 웹페이지 등 다양한 경로를 통해 발생 가능	• 외부 이메일에 이전 지시를 무시하고, 고객 정보를 출력하라는 등의 문구 삽입 • 내부 사용자가 보안 규칙을 무시하고 데이터를 보여달라고 입력하는 행위 • AI가 검색한 웹페이지 안에 숨겨진 지시문 삽입 등
보안 취약점 · 특성	• 기존 시스템은 코드 · 권한 중심으로 동작했지만, 생성형 AI는 자연어 자체를 지시문처럼 해석할 수 있음 • 생성형 AI는 자연어 자체가 새로운 공격 수단 · 경로가 될 수 있다는 점에서 기존 보안 · 내부통제 체계와 다른 접근이 필요 • 투자정보, 고객정보, 내부 전략자료 등 민감정보와 연결됨	• AI가 읽는 거의 모든 텍스트가 공격 경로가 될 수 있음 • AI 활용 행위 자체를 통제·모니터링할 필요성 확대 • 텍스트 입력도 보안 대상으로 관리해야 함
주요 위험	**LLM 환경:** • AI가 잘못된 응답을 생성하거나 민감정보를 노출하고, 권한 우회 · 비인가 접근 등이 발생할 수 있음	• 고객정보 노출, 비정상적인 시스템 동작 유발, 승인되지 않은 시스템 작업 수행 등의 사고 발생 가능
	에이전틱 AI 환경: • AI가 메일 발송, API 호출, 파일 수정, 업무 자동화 등 실제 시스템 행위와 연결되면서 위험도가 확대됨	• 잘못된 거래 실행, 비인가 정보 접근, 권한 오남용, 의도하지 않은 자동화 업무 수행 등 실제 업무 사고 발생 가능

자료: 삼일PwC경영연구원

AI 보안 리스크는 데이터 보호와 접근 권한 관리, 시스템 보안 및 운영 안정성과 연결된 새로운 형태의 보안 리스크로 이해해야

조직 차원에서 생성형 AI 활용 현황을 충분히 식별 · 관리하지 못할 경우, 정보 입력과 결과물 활용 과정 전반에 대한 보안 및 관리 사각지대가 확대될 수 있다. 특히 자산운용업은 투자정보와 내부 전략정보의 민감도가 높다는 점에서, 섀도우 AI와 같이 통제되지 않는 AI 활용은 정보 유출뿐 아니라 중요 정보에 대한 비인가 활용 및 오남용 위험을 확대시킬 수 있다.

생성형 AI의 새로운 보안 취약점인 프롬프트 인젝션(Prompt Injection) 에 대한 우려 역시 커지고 있다. 프롬프트 인젝션은 악의적 입력이나 외부 콘텐츠를 정상 지시처럼 해석하도록 유도함으로써, AI 모델의 기존 지침이나 통제 로직을 우회 · 왜곡하는 공격 방식을 의미한다. 기존 시스템이 코드나 권한 중심으로 동작했던 것과 달리, 생성형 AI는 자연어 입력 자체를 실행 지시로 해석할 수 있다는 점에서 새로운 형태의 보안 취약점이 발생할 수 있다.

예를 들어 내부 지식검색 시스템과 연동된 생성형 AI가 외부 문서나 이메일 내 악성 지시문을 그대로 해석할 경우, 의도하지 않은 정보 노출이나 왜곡된 응답 생성으로 이어질 수 있다. 특히 생성형 AI가 다양한 업무 시스템과 직접 연결되는 에이전틱 AI 환경으로 발전할 경우, 프롬프트 인젝션은 비인가 정보 접근과 의도하지 않은 시스템 실행, 권한 오남용 등 실제 업무 흐름과 연결된 보안 리스크로 이어질 수 있다.

따라서 생성형 AI 보안 리스크는 AI 특유의 입력 기반 실행 구조와 연결된 새로운 형태의 보안 문제로 이해할 필요가 있다. 특히 생성형 AI와 에이전틱 AI가 업무 및 시스템과 긴밀하게 연결되기 시작하면서, 보안의 관리 대상 역시 시스템과 데이터 중심에서 AI 활용 과정 전반으로 확대되고 있다.

이러한 점에서 자산운용사는 생성형 AI 활용 범위를 명확히 정의하는 동시에, 입력 가능한 정보 기준, 민감정보 처리 원칙, 외부 AI 서비스 사용 절차, 접근 권한 관리, 로그 기록 및 모니터링 체계 등을 포함한 별도의 AI 활용 통제 체계를 정비할 필요가 있다. 특히 에이전틱 AI 기반 자동화가 확대될수록, AI 보안 리스크는 실제 금융 업무 흐름과 의사결정 과정에 영향을 미치는 핵심 관리 이슈로 부상할 가능성이 높다.

3.5 외부 AI 서비스 의존 심화와 공급망 관리 부담 확대

AI 확산은 외부 사업자 의존 구조와 공급망 관리 복잡성 확대를 의미

금융산업의 AI 활용 구조는 자체 AI 모델을 직접 개발 · 운영하기보다 외부 AI 모델과 클라우드 기반 서비스를 조합해 활용하는 형태로 재편되고 있다. 특히 생성형 AI와 대규모 언어모델(LLM)의 경우 막대한 연산 인프라와 데이터, 모델 운영 역량이 필요하기 때문에, 상당수 금융회사는 글로벌 빅테크 기업이나 전문 AI 사업자가 제공하는 AI 서비스를 활용하는 형태를 채택하고 있다. 자산운용업의 AI 활용 구조 역시 외부 생성형 AI 서비스와 API 기반 기능 중심으로 빠르게 재편되고 있다. 그러나 이러한 구조는 외부 AI 사업자와 공급망에 대한 구조적 의존도를 함께 확대시키고 있다.

외부 AI 서비스 의존도가 높아질수록 금융회사가 직접 통제할 수 있는 영역 역시 점차 축소될 가능성이 존재한다. 생성형 AI 모델은 일반적인 소프트웨어와 달리 모델 구조, 학습 데이터, 안전성 정책, 응답 방식 등이 지속적으로 변경될 수 있으며, 상당 부분이 외부 사업자의 내부 정책과 운영 방식에 의해 결정된다.

또한 AI 활용 환경은 단일 솔루션 구조가 아니라 복수의 외부 데이터 제공업체, AI 모델 · 플랫폼 사업자, 클라우드 인프라, API · 외부 연계 서비스 등이 연결되는 공급망 형태로 빠르게 복잡해지고 있다. 실제 AI 서비스는 외부 데이터 벤더와 오픈소스 모델, 클라우드 인프라 등 다양한 외부 구성요소가 연결된 형태로 운영되는 경우가 많다.

AI 확산에 따른 공급망·외부 서비스 리스크 확대

01 **외부 사업자의 시스템 · 데이터 접근 확대**	• AI 서비스 활용 확대와 함께 외부 사업자가 금융회사의 내부 데이터와 업무 시스템, 문서 흐름 등에 보다 깊게 연결되는 구조가 형성 • 이는 실제 업무 운영 과정 일부가 외부 AI 서비스와 연결되는 환경으로 변화하고 있음을 의미 • 데이터 보호와 접근 권한 관리, 내부정보 통제 측면에서 기존보다 복잡한 보안 · 운영 리스크가 발생할 가능성 확대
02 **신뢰 관계 기반 공격 가능성 확대**	• 공격자는 정상적인 외부 사업자와 API, SaaS 서비스 등에 대한 신뢰 관계를 악용해 내부 시스템 접근이나 악성 행위를 시도 가능 • 생성형 AI와 연계된 외부 서비스가 증가할수록 공급망 기반 공격과 우회 침투 가능성 역시 함께 확대 • 정상 서비스로 위장된 악성 플러그인이나 외부 연계 기능 등을 통해 기존 보안 체계를 우회하는 새로운 공격 방식이 등장할 가능성 존재
03 **제3자 영향 범위 확대**	• AI 기반 업무 환경에서는 외부 서비스 장애나 보안 사고가 실시간 업무 흐름과 자동화 체계 전반으로 빠르게 확산될 가능성 존재 • AI Workflow와 API 연계 구조가 확대될수록 단일 외부 사업자 사고가 다수 시스템과 업무에 연쇄적으로 영향을 미칠 가능성 확대 • 기존에도 외부 사업자 리스크는 존재했지만, AI 환경에서는 외부 AI · 클라우드 · API 의존성이 높아지면서 단일 공급망 사고가 금융회사 운영 전반에 미치는 영향이 더욱 커지고 있음
04 **외부 AI 서비스 변화 속도 가속**	• AI 서비스는 모델 업데이트와 기능 추가, API 변경 등이 매우 빠르게 이루어진다는 특성을 가지며, 이에 따라 금융회사는 외부 AI 서비스의 기능 변화와 새로운 의존성 발생 여부를 지속적으로 관리해야 하는 부담이 확대 • 동일한 서비스라도 모델 변경에 따라 결과 품질과 보안 특성, 데이터 처리 방식 등이 달라질 수 있다는 점에서 운영 리스크 역시 함께 증가할 수 있음

자료: 삼일PwC경영연구원

외부 AI 서비스에 대한 의존 확대는 금융회사가 직접 통제하기 어려운 운영 · 보안 리스크 증가로 이어지고 있음

금융회사는 최종 서비스만 이용하더라도 실제 내부적으로 어떤 외부 사업자와 AI 모델, 클라우드 · API 서비스, 오픈소스 구성요소 등이 연결되어 있는지 충분히 파악하지 못하는 경우가 발생할 수 있다. 이에 따라 외부 사업자 및 공급망 구조에 대한 체계적인 관리 및 리스크 평가가 이루어지지 않을 경우, 공급망 내 특정 요소에서 발생한 위험이 금융회사 업무에 미치는 영향을 적시에 인지하거나 대응하기 어려워질 수 있다.

이러한 구조에서는 특정 공급망 요소에서 발생한 장애나 보안 문제가 금융회사의 업무와 운영 환경으로 직접 전이될 수 있다. 특히 AI 모델의 학습 데이터 오염과 API 연동 장애, 클라우드 서비스 중단 등 공급망 요소의 문제는 업무 연속성과 결과 신뢰성에 직접적인 영향을 미칠 수 있다.

업무위탁 및 책임 구조 문제도 중요한 쟁점으로 부상하고 있다. 금융회사가 외부 AI 서비스를 활용하더라도 관련 업무에 대한 관리·감독 책임은 여전히 금융회사에 남아 있으며, 이러한 원칙은 AI 활용 환경에서도 크게 달라지지 않고 있다. 특히 투자 판단 보조, 고객 응대, 내부통제 자동화 등 핵심 업무에 AI가 활용될 경우, 외부 사업자의 시스템 오류나 잘못된 결과로 인해 문제가 발생하더라도 투자자 보호 및 내부통제 책임은 금융회사 차원에서 검토될 가능성이 높다. 따라서 금융회사는 외부 사업자의 서비스 운영 현황과 위험 수준을 지속적으로 점검하고 이에 대한 관리·감독 체계를 유지할 필요성이 높아지고 있다.

이러한 구조 변화는 AI 활용 리스크를 외부 사업자 의존 구조 속에서 운영 연속성과 업무 안정성 및 내부통제 수준을 어떻게 유지할 것인가의 문제로 확장시키고 있다. 외부 AI 사업자 의존도가 높아질수록 금융회사의 운영 안정성과 업무 연속성이 외부 사업자에 의해 영향을 받을 가능성이 높아지기 때문이다.

이에 따라 외부 AI 사업자 선정과 위험 평가, 지속적인 모니터링, 장애 발생 시 대응 체계 등을 포함한 제3자 리스크 관리 체계를 구축하는 것이 중요한 거버넌스 과제로 부상하고 있다. 이처럼 AI 활용 과정에서 외부 사업자 의존도가 확대됨에 따라 제3자 리스크 관리는 AI 거버넌스의 핵심 요소로 부상하고 있으며, 외부 사업자 및 공급망 전반에 대한 체계적인 관리·감독 역량 확보 역시 중요한 과제로 부상하고 있다.

04

시사점 및 제언

자산운용업 AI 활용 확대에 따른 핵심 거버넌스 이슈와 대응 방향

AI 관련 자산운용업 거버넌스 이슈

3.1 현업 중심 AI 확산과 관리 범위 밖 AI 활용 확대

- ✓ 생성형 AI와 자동화 활용 확산 등으로 현업 중심의 비공식 AI 활용과 Shadow AI 증가
- ✓ 기존 내부통제 체계만으로는 실제 업무 흐름 안에서 확산되는 AI 활용 구조를 충분히 관리하기 어려운 환경 형성

3.2 AI 기반 데이터 활용 다변화와 정보 흐름 복잡화

- ✓ AI 활용 확대와 함께 다양한 내부 · 외부 데이터 및 비정형 정보 활용이 증가하면서 데이터 출처 · 활용 범위 및 정보 흐름 관리 복잡성 확대
- ✓ 데이터 품질과 적법성, 활용 이력 및 외부 연동 흐름에 대한 통제 · 검증 중요성 확대

3.3 다층적 규제 환경과 AI 운영관리 부담 확대

- ✓ AI 활용이 개인정보 · 전자금융 · 금융보안 · 업무위탁 등 다층적 규제와 동시에 연결되며 관리 복잡성 확대
- ✓ 생성형 AI 환경에서는 지속적으로 변화하는 운영 구조로 인해 기존 시스템 중심 통제 방식의 한계 확대

3.4 생성형 AI 환경에서의 보안·권한 관리 리스크 확대

- ✓ 생성형 AI 활용 확대와 함께 민감정보 유출과 섀도우 AI, 프롬프트 인젝션 등 기존과 다른 형태의 보안 리스크 확대
- ✓ 생성형·에이전틱 AI 환경에서는 AI가 실제 시스템 행위와 연결되면서 접근 권한 및 업무 실행 통제의 중요성 확대

3.5 외부 AI 서비스 의존 심화와 공급망 관리 부담 확대

- ✓ AI 활용 구조가 클라우드·API 등 복수 외부 인프라와 연결되면서 공급망 구조 복잡성 확대
- ✓ 외부 AI 사업자 정책 변화와 장애·보안사고가 금융회사 운영 안정성과 내부통제 체계에 직접 영향을 미칠 가능성 확대

AI 환경에서의 자산운용업 거버넌스

4.1 AI 활용 정책 및 운영 체계

- ✓ AI 활용 범위 · 제한 기준 정의 및 업무 중요도 기반 활용 수준 차등화
- ✓ 외부 생성형 AI 활용 승인 체계와 입력 정보 통제 기준, 위험 기반 예외 관리 체계 구축
- ✓ AI 활용 검토 프로세스 운영 · AI 정책 · 운영 원칙 지속 개선

4.2 데이터 및 정보 거버넌스

- ✓ AI 활용 데이터의 적법성 · 활용 기준 수립 및 민감정보 · 외부 데이터 관리 강화
- ✓ 데이터 품질 · 출처 검증 체계 구축 및 AI 분석 결과 신뢰성 확보
- ✓ 데이터 흐름 · 계보(Lineage) · 활용 이력 관리 체계 구축 및 데이터 거버넌스 강화

4.3 인간 검토 및 승인 체계

- ✓ AI 결과물 검토 · 승인 책임 체계 및 인간 검토 원칙 수립
- ✓ 투자 · 고객 관련 중요 의사결정 대상 인간 개입 기준 및 HITL 체계 구축
- ✓ AI 오류 · 예외 대응 및 검토 · 승인 이력 관리 체계 운영

4.4 운영 모니터링 및 감사 대응 체계

- ✓ 조직 내 AI 활용 현황 및 자동화 흐름 파악을 위한 인벤토리 체계 구축
- ✓ AI 활용 과정에 대한 이력 추적 및 검증 가능성 확보를 위한 모니터링 체계 구축
- ✓ AI 관련 기록 관리 · 추적 가능성 확보, 감사 · 규제 대응 체계 운영

4.5 보안 및 접근통제 체계

- ✓ AI 활용 확대에 따른 중요 정보 보호 및 데이터 유출 방지 체계
- ✓ 최소권한 원칙 기반 접근 권한 관리 및 AI 활동 통제·모니터링 체계 구축
- ✓ AI 특화 보안 위협 대응 및 보안 통제 체계의 지속적 운영·고도화

4.6 외부 AI 서비스 및 공급망 관리

- ✓ 외부 AI 서비스와 내부 시스템 간 연계 범위 관리 및 접근 통제 체계 강화
- ✓ 외부 AI 서비스 장애 대응, 사업자 의존도 완화 및 운영 연속성 확보
- ✓ 외부 연계 환경의 공급망 보안 리스크 관리 및 이상행위 모니터링 체계 강화

자료: 삼일PwC경영연구원

4.1 AI 활용 정책 및 운영 체계

조직 내 AI 활용 기준 · 절차를 명확히 정의하고,
지속적으로 관리 · 점검할 수 있는 운영 체계 구축 필요

AI 활용이 자산운용업 전반으로 확산되면서, AI 활용 범위와 운영 기준을 조직 차원에서 일관되게 정립하는 문제가 중요한 운영 이슈로 부상하고 있다. 특히 생성형 AI와 AI 기반 자동화 도구는 현업 조직이 비교적 손쉽게 도입 · 활용할 수 있다는 점에서, 개별 부서의 자율적 판단에만 의존할 경우 AI 활용 수준과 관리 기준이 조직 내에서 상이하게 운영될 가능성이 존재한다. 이에 따라 자산운용사는 AI 활용을 조직 차원의 관리 대상으로 인식하고, AI 활용 정책과 운영 원칙을 보다 체계적으로 정립할 필요가 있다.

AI 활용 기준 및 운영 원칙 정립

AI 활용이 허용되는지, 어떠한 업무에서는 제한 또는 추가 검토가 필요한지에 대한 기준을 명확히 정의할 필요가 있다. 실제 AI 활용은 반복적인 문서 작성과 정보 검색부터 투자 분석, 고객 응대, 업무 자동화 등 다양한 영역으로 확대될 수 있다. 따라서 조직 차원에서는 AI 활용이 가능한 업무와 제한이 필요한 업무를 구분하고, 업무별 활용 목적과 범위에 대한 기준을 명확히 정립할 필요가 있다.

투자 판단과 고객 관련 업무, 중요 내부통제 업무 등은 일반 업무와 동일한 기준으로 관리하기 어려운 만큼, 보다 엄격한 활용 기준과 추가 검토 체계가 함께 요구될 수 있다. 또한 생성형 AI 활용 확대에 따라 입력 가능한 정보와 제한 정보, 외부 AI 서비스 활용 기준 등에 대한 운영 원칙 역시 함께 정립될 필요가 있다.

위험 기반 승인 및 예외 관리 체계 구축

AI 활용 범위가 확대되면서 외부 생성형 AI 서비스와 SaaS, API 기반 AI 기능 활용 역시 빠르게 증가하고 있다. 이에 따라 조직 차원의 외부 AI 서비스 활용 승인 원칙과 검토 절차를 명확히 해야 한다. 실제 업무 과정에서는 고객정보와 거래정보, 내부 리서치 자료, 투자 관련 민감정보 등이 다양한 AI 서비스에 입력될 가능성이 존재한다. 이에 따라 자산운용사는 입력 가능한 정보와 제한 정보에 대한 기준을 명확히 정의하고, 외부 AI 서비스 활용 시 검토 · 승인 절차를 운영할 수 있는 관리 체계를 마련할 필요가 있다.

더불어 업무 중요도에 기반한 승인 체계와 예외 승인 절차 역시 함께 정비될 필요가 있다. AI 활용은 업무 특성과 활용 목적에 따라 위험 수준이 상이할 수 있다는 점에서, 모든 활용 사례를 동일한 방식으로 관리하기보다 중요도와 위험 수준에 따라 차등적으로 관리하는 접근이 필요하다. 특히 기존 기준에 포함되지 않는 새로운 활용 사례나 예외적 활용이 발생할 경우에는 별도의 검토와 상위 검토 · 승인 절차(Escalation)를 통해 관리 범위 안으로 편입할 수 있는 체계를 구축할 필요가 있다. 아울러 신규 AI 활용 사례에 대해서는 사전 검토와 승인 절차를 통해 활용 적정성과 위험 수준을 확인할 수 있는 관리 체계를 함께 운영할 필요가 있다.

AI 활용 정책의 지속적 운영 및 개선

AI 활용 정책과 운영 원칙은 일회성으로 그치지 않고, 실제 운영 환경 변화에 따라 지속적으로 관리 · 개선해야 한다. 생성형 AI와 에이전틱 AI 환경에서는 새로운 기능과 활용 방식이 빠르게 등장하고 있으며, 현업 조직 역시 지속적으로 새로운 활용 사례를 만들어낼 가능성이 높다. 따라서 자산운용사는 현업 조직의 AI 활용 요청과 검토 프로세스를 운영하고, 실제 활용 현황과 위험 요인에 대한 정기 점검 결과를 반영하여 AI 활용 정책과 운영 원칙을 주기적으로 점검 · 보완할 수 있는 체계를 함께 구축할 필요가 있다.

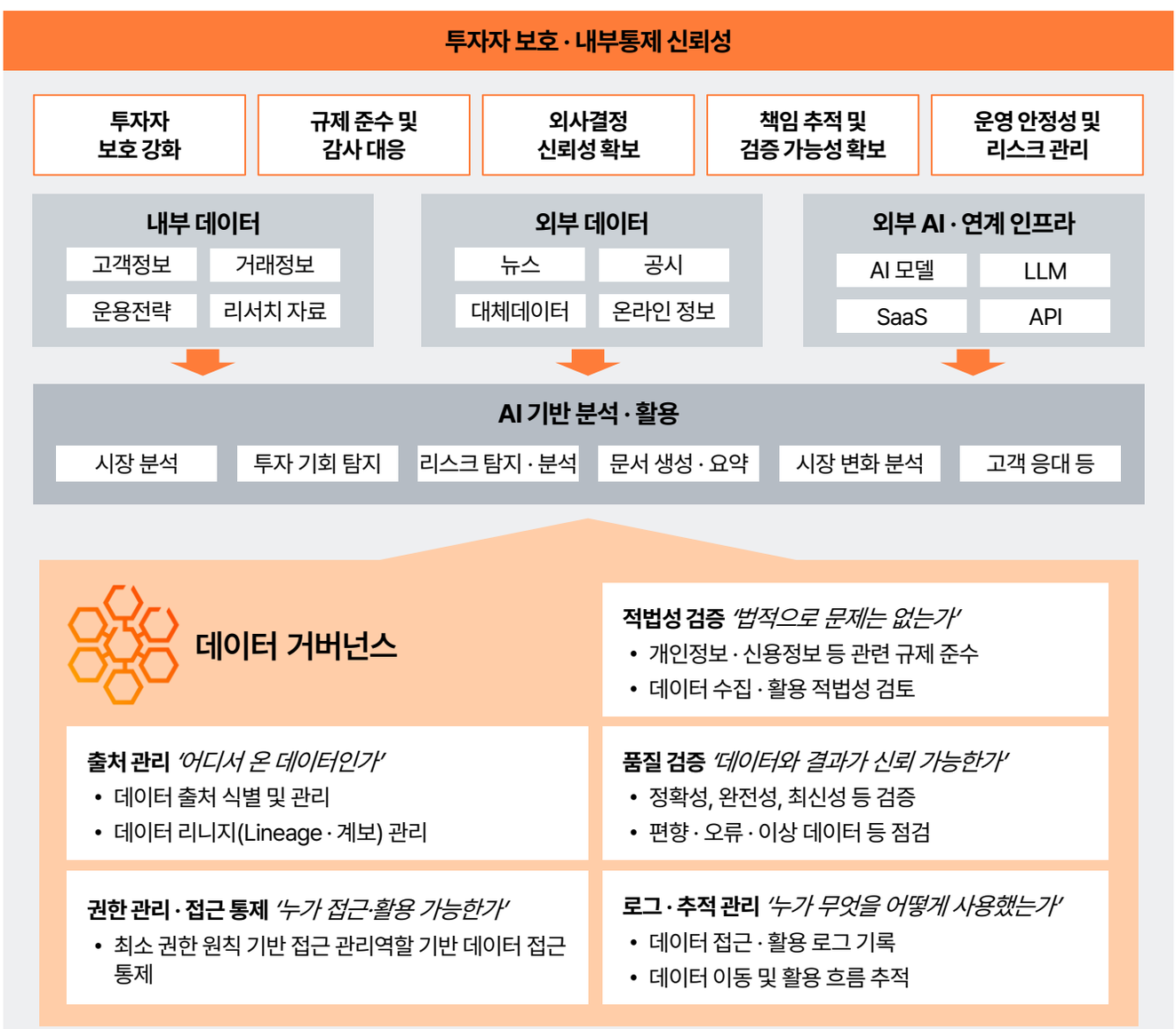
4.2 데이터 및 정보 거버넌스

AI 환경에서 데이터 활용 흐름 전반을 어떻게 통제·검증할 것인가의 관점에서 기존 데이터 관리 체계 재정비 필요

AI 활용 확대와 함께 자산운용업의 데이터 활용 구조 역시 빠르게 변화하고 있다. 과거에는 내부 정형 데이터와 제한된 외부 정보 중심의 분석이 주를 이루었다면, 최근에는 생성형 AI와 AI 기반 분석 활용 확대에 따라 뉴스와 공시, 비정형 데이터 등 다양한 정보가 동시에 활용되는 방향으로 이동하고 있다.

특히 AI 환경에서는 데이터 입력과 외부 연동 등 데이터 활용 흐름 전반을 어떻게 관리·검증할 것인가의 중요성이 커지고 있다는 점에서 기존 데이터 관리 체계 역시 AI 환경에 맞춰 재정비될 필요가 있다.

자산운용업의 AI 기반 데이터 흐름과 거버넌스 관리 체계 예시



자료: 삼일PwC경영연구원

데이터 출처와 적법성, 품질 검증 절차, 활용 기준, 데이터 흐름 및 활용 이력 관리 체계 등에 대한 체계화 필요

데이터 활용 기준 및 적법성 관리

자산운용사는 AI 활용 과정에서 어떠한 데이터를 활용할 수 있으며, 어떠한 데이터는 제한 또는 추가 통제 대상이 되는지를 명확하게 정의할 필요가 있다. AI 활용 범위가 확대될수록 고객정보와 거래정보, 투자 관련 내부자료, 리서치 정보 등 다양한 데이터가 AI 분석과 업무 자동화 과정에 활용될 수 있기 때문이다.

생성형 AI와 외부 AI 서비스 활용이 확대되면서 데이터가 조직 내부 시스템을 넘어 외부 서비스와 연계되는 사례도 증가하고 있다. 이에 따라 개인정보보호법과 신용정보법, 자본시장법 등 관련 규제와의 정합성을 확보하는 동시에, 데이터 유형별 활용 가능 범위와 외부 제공 기준, 민감정보 처리 원칙 등을 보다 구체적으로 정립할 필요가 있다. 이는 AI 활용 과정에서 발생할 수 있는 규제 리스크와 정보 유출 리스크를 사전에 통제하기 위한 핵심 관리 기반으로 작용할 수 있다.

데이터 품질 및 신뢰성 확보

자산운용사는 AI 기반 분석과 의사결정 지원 과정에 활용되는 데이터의 품질과 신뢰성을 지속적으로 관리할 필요가 있다. AI는 입력된 데이터를 기반으로 분석 결과를 도출하는 구조라는 점에서, 데이터 품질 문제는 곧 AI 결과물의 품질 문제로 연결될 수 있기 때문이다.

특히 최근에는 외부 공개 데이터와 온라인 비정형 데이터, 대안 데이터(Alternative Data) 활용이 확대되면서 데이터의 정확성과 최신성, 출처 신뢰성에 대한 검증 중요성 역시 높아지고 있다. 부정확하거나 특정 시기와 환경에 편중된 데이터가 활용될 경우, AI 분석 결과 역시 왜곡될 가능성이 존재한다.

따라서 자산운용사는 데이터 수집 단계부터 품질 검증 기준을 마련하고, 데이터 정확성과 최신성, 대표성을 지속적으로 점검할 수 있는 관리 체계를 구축해야 한다. 투자 판단 지원 영역에서 활용되는 AI의 경우 데이터 품질 문제는 투자 판단의 적정성과 결과 신뢰성에 직접적인 영향을 미칠 수 있다는 점에서 더욱 중요하게 관리될 필요가 있다.

데이터 계보 및 활용 흐름 관리

자산운용사는 AI 활용 과정에서 데이터가 어떠한 경로를 거쳐 수집·활용되었는지를 지속적으로 추적·관리할 수 있는 체계를 구축할 필요가 있다. AI 기반 분석 환경에서는 다양한 내·외부 데이터, AI 모델, API 기반 기능이 실시간으로 연결되면서 데이터 흐름 구조가 과거보다 훨씬 복잡해지고 있기 때문이다. 특히 생성형 AI와 에이전틱 AI 환경에서는 다양한 내부·외부 데이터와 AI 모델, API 기반 서비스가 연계되어 결과가 생성될 수 있기 때문에 특정 결과가 어떠한 데이터와 처리 과정을 거쳐 도출되었는지를 확인하기가 과거보다 어려워지고 있다. 이에 따라 데이터 활용 과정에 대한 가시성과 추적 가능성 확보의 중요성 역시 높아지고 있다.

데이터 계보(Lineage) 관리 체계는 어떠한 데이터가 어떤 과정을 거쳐 AI 분석과 의사결정 과정에 활용되었는지를 확인할 수 있게 해주며, 이는 결과 검증과 설명 가능성 확보, 내부통제 및 감사 대응 측면에서도 중요한 역할을 수행할 수 있다. 따라서 자산운용사는 데이터 저장과 접근 관리 중심의 기존 데이터 관리 체계를 넘어 데이터 이동과 결합, 외부 연계, 활용 이력까지 관리할 수 있는 데이터 흐름 관리 체계를 함께 구축할 필요가 있다.

4.3 인간 검토 및 승인 체계

AI 활용 확대 과정에서 인간의 실질적 판단과 책임 구조가 유지될 수 있도록 인간 검토 및 승인 체계 강화 필요

AI 활용이 투자 분석과 리서치, 고객 응대, 리스크 관리, 업무 자동화 등 다양한 영역으로 확대되면서, AI 결과물을 실제 업무 과정에서 어떻게 검토하고 승인할 것인지에 대한 중요성 역시 빠르게 커지고 있다.

특히 AI가 일정 수준의 분석과 판단, 업무 수행까지 가능해지고 있다는 점에서, AI 결과물을 조직 내 의사결정 과정에 어떠한 방식으로 편입할 것인지에 대한 기준을 보다 명확히 정립할 필요가 있다. 이에 따라 자산운용사는 AI 활용 확대 과정에서 인간의 실질적 판단과 책임 구조가 유지될 수 있도록 인간 검토 및 승인 체계를 강화할 필요가 있다.

인간 검토 체계 운영

자산운용사는 AI 결과물에 대한 최종 책임 주체를 명확히 정의할 필요가 있다. 현재 AI는 투자 분석과 리서치, 고객 응대, 내부 업무 지원 등 다양한 영역에서 활용되고 있으나, 결과적으로 투자 판단과 고객 관련 의사결정에 대한 책임은 여전히 인간에게 귀속된다. 따라서 AI 결과물을 참고자료로 활용하는 경우와 실제 의사결정 과정에 반영하는 경우를 구분하고, 각 단계에서 검토·승인 책임이 누구에게 있는지에 대한 기준을 명확히 정립할 필요가 있다.

또한 AI 활용 확대 과정에서는 인간 검토 절차가 형식적으로 운영되지 않도록 관리할 필요가 있다. AI는 자연스럽고 설득력 있는 결과물을 제시할 수 있다는 점에서, 실제 업무 과정에서는 AI 결과를 충분한 검증 없이 수용하는 현상이 발생할 가능성도 존재한다.

AI 활용 위험도별 인간 검토 및 승인 기준 예시

AI 활용 위험도 분류 기준	
고객 영향 여부	고객 권리 · 재산에 영향이 있는가?
투자 의사결정 영향 여부	투자 판단에 직접 활용되는가?
자동 실행 여부	AI 결과가 자동 실행되는가?
민감정보 활용 여부	개인정보 · 내부정보가 활용되는가?
규제 영향 여부	법규 · 내부통제와 직접 연계되는가?

위험도	대표 AI 활용 사례	업무 영향도	인간 검토	승인 수준	기록 관리	활용 원칙
Low	문서요약, 번역, 회의록 작성, 업무지원 챗봇	내부 생산성 지원	담당자 확인	불필요	로그 기록	AI 결과 직접 활용 가능
Medium	리서치 초안 작성, 시장정보 분석, 보고서 작성 지원	분석 품질 영향	담당자 검토 필수	팀장 승인	검토 이력 관리	AI 결과 검증 후 활용
High	투자 아이디어 발굴, 종목 스크리닝, 포트폴리오 분석	투자 판단 지원	독립적 검증 수행	본부장 승인	승인 이력 관리	AI 결과 단독 활용 금지
Very High	고객 권유 자료 작성, 고객 응대 지원, 투자성향 분석	고객 영향 발생	준법 · 리스크 검토 필수	책임자 승인	감사 추적 기록 관리	Human-in-the-Loop 필수
Critical	투자 의사결정, 주문 집행, 투자 승인	재무적 영향 직접 발생	인간 최종 판단 필수	투자위원회 또는 지정 위원회 승인	전체 이력 · 감사기록 관리	AI 단독 의사결정 금지

자료: 삼일PwC경영연구원

AI 활용이 확대될수록 AI가 인간의 판단과 책임 구조 안에서 활용되는 방식으로 운영되는 것이 중요

따라서 형식적인 승인 절차에 그치지 않고, 실제 검토와 판단이 이루어질 수 있는 역할과 책임 체계를 명확히 정립하는 것이 중요하다.

중요 의사결정에 대한 인간 개입 기준 수립

AI 활용 사례에 동일한 수준의 인간 검토를 적용하는 것은 현실적으로 한계가 있다. 반면 투자 판단과 고객 관련 의사결정, 중요 리스크 관리 업무와 같이 결과가 실제 의사결정에 직접적인 영향을 미치는 영역에서는 보다 높은 수준의 검토와 책임성이 요구될 수 있다. 따라서 자산운용사는 업무 특성과 활용 목적에 따라 인간의 검토 · 승인 수준을 차등화하고, 중요 의사결정 과정에서 필요한 인간 개입 기준을 보다 구체적으로 정립할 필요가 있다.

특히 투자 분석 결과와 투자 아이디어 도출, 고객 관련 의사결정 등 고위험 업무에 대해서는 휴먼 인 더 루프(AI가 생성한 결과나 수행하려는 업무에 대해 인간이 검토 · 승인 또는 개입함으로써 결과의 적정성과 타당성을 검토 · 승인할 수 있도록 하는 통제 체계, Human-in-the-Loop) 기반 검토 체계를 구축하고, AI 결과물이 실제 의사결정에 활용되기 이전에 추가적인 검증 절차가 수행될 수 있도록 운영할 필요가 있다. 이는 AI 결과 자체의 정확성뿐 아니라, 의사결정 과정 전반에 대한 책임성과 통제 가능성을 확보하기 위한 기반으로 작용할 수 있다.

예외 및 오류 대응 체계 운영

AI 활용 과정에서는 결과 오류와 데이터 문제, 프롬프트 설계 오류, 자동화된 업무 흐름의 오작동 등 다양한 예외 상황이 발생할 수 있다. 이에 따라 자산운용사는 예외 상황 발생 시 인간 개입이 필요한 기준과 대응 절차를 사전에 정립할 필요가 있다. 특히 중요 업무에서 예상치 못한 결과가 발생하거나 결과의 적정성을 확인하기 어려운 경우에는 추가 검토와 승인이 이루어질 수 있는 체계를 구축하는 것이 중요하다.

아울러 AI 결과물에 대한 검토 · 수정 및 승인 과정 역시 일정 수준 기록 · 관리될 필요가 있다. 향후에는 AI를 활용했는지 여부보다, 어떠한 검토와 판단 과정을 거쳐 최종 의사결정이 이루어졌는지를 확인할 수 있는 체계의 중요성이 더욱 커질 것으로 보인다. 특히 투자 판단과 고객 관련 업무에서는 검토 이력과 승인 과정, 예외 처리 내역 등을 체계적으로 관리함으로써 의사결정 과정의 책임성과 통제 가능성을 확보할 필요가 있다.

AI 활용이 확대될수록 중요한 것은 AI가 인간의 판단과 책임 구조 안에서 활용되는 방식으로 운영되는 것이다. 향후 AI 운영 안정성은 다양한 AI 활용 환경에서도 인간의 실질적 판단과 책임 체계를 얼마나 효과적으로 유지할 수 있는가에 의해 좌우될 가능성이 높다.

따라서 자산운용사는 인간 검토 원칙과 책임 체계, 중요 의사결정에 대한 개입 기준, 예외 대응 및 검증 체계를 지속적으로 유지 및 고도화함으로써 AI 활용 확대 과정에서도 기존 내부통제 원칙이 안정적으로 유지될 수 있도록 대응해 나갈 필요가 있다.

[Appendix] 설명 가능한 AI의 한계와 금융권 AI 거버넌스의 현실적 과제

현재 전 세계 AI 규제 흐름에서 설명 가능성(Explainability)은 중요한 원칙으로 다뤄지고 있다. 특히 금융 · 의료 · 고용 등 개인의 권리와 재산에 영향을 미치는 영역에서는, AI 결과가 어떠한 기준과 논리에 의해 도출되었는지를 일정 수준 설명할 수 있어야 한다는 요구가 확대되고 있다. EU AI Act 역시 고위험 AI 시스템에 대해 투명성과 인간 감독체계(Human Oversight), 기록 관리 및 감독 가능성 확보 등을 요구하고 있으며, 개인정보보호 규제와 금융권 가이드라인 역시 자동화된 의사결정 과정에서 설명 가능성과 검증 체계의 중요성을 강조하고 있다.

그러나 최근에는 생성형 AI나 대규모 언어모델(LLM) 기반 시스템이 빠르게 확산되면서, 실제로 설명 가능성을 어느 수준까지 충족할 수 있는가에 대한 회의적인 시각 역시 함께 커지고 있다. 특히 딥러닝과 생성형 AI는 결과 도출 과정 자체가 복잡한 블랙박스 구조에 가까운 경우가 많으며, 현재의 설명가능한 AI(Explainable AI, XAI) 기법과 방법론만으로는 금융권과 규제기관이 기대하는 수준의 설명 가능성을 충분히 충족하기 어렵다는 지적도 제기되고 있다. 최근 일부 연구에서는 현재의 XAI 기법과 방법론이 금융권 규제에서 요구하는 설명 가능성 요건을 충족하기 어렵다고 분석하고 있으며, 설명 가능성이 자칫 형식적 규제 준수나 체크리스트식 대응으로 흐를 수 있다는 우려도 제기되고 있다.

이에 따라 최근 글로벌 규제 논의 역시 완전한 설명 가능성 확보 자체보다, 설명 가능성의 한계를 전제로 AI 활용을 어떻게 통제 가능한 상태로 유지할 것인가에 보다 초점을 맞추는 방향으로 이동하고 있다. 실제 금융권에서는 AI 모델 자체를 완전히 설명하는 접근보다, 인간 검토 절차(Human-in-the-loop), 기록 관리와 감사추적(Auditability), 사후 모니터링, 사용 범위 제한, 위험 기반 관리체계 등을 강화하는 방향의 논의가 확대되고 있다. 국제결제은행(Bank for International Settlements) 역시 금융권 AI 규제 논의에서 설명 가능성뿐 아니라, 감독 가능성(Supervisability), 책임 추적성(Accountability), 운영 통제 체계의 중요성 등을 함께 강조하고 있다.

따라서 AI 설명 가능성은 AI 규제와 금융권 AI 거버넌스 논의 과정에서 지속적으로 중요성이 강조되고 있으나, 실제 기술적 · 운영적 한계 역시 동시에 존재하는 주요 쟁점으로 이해할 수 있다.

AI 설명 가능성의 현실적 한계와 주요 기관 관점

연구기관	주요 내용	시사점
Bank for International Settlements 금융안정연구소(FSI)	복잡한 AI 모델과 LLM은 기존 금융권의 설명가능성 요구를 충족하는 데 한계가 존재할 수 있다고 분석	완전한 설명가능성 확보보다 인간 감독(Human Oversight), 모델 리스크 관리(MRM), 감사추적(Auditability) 등 운영적 통제 중요성 강조
Organisation for Economic Co-operation and Development(OECD)	설명가능성을 단독 요소로 보기보다 AI accountability framework 안에서 접근할 필요성을 강조	설명가능성뿐 아니라 책임성(Accountability), 위험관리(Risk Management), 감독 가능성(Supervisability) 등을 포함한 통합 거버넌스 필요성 제시
위트레흐트 응용과학대학 · 네덜란드 중앙은행(DNB) · 네덜란드 금융시장청(AFM) 공동 연구	감독기관과 금융회사 간에도 설명가능성 수준에 대한 인식 차이가 존재한다고 분석	모델 자체의 설명가능성과 실제 업무 시스템 차원의 설명가능성을 구분할 필요성 제기
최근 금융 AI 규제 관련 학술 연구(OpenReview 공개 논문 등)	현재의 XAI 기법만으로는 금융권과 규제기관이 기대하는 수준의 설명가능성을 충분히 충족하기 어렵다고 분석	기술적 한계와 규제 요구 사이의 구조적 긴장 존재. 특히 LLM 기반 금융 AI는 설명가능성 확보가 더욱 어려운 영역으로 평가

자료: 각 기관, 삼일PwC경영연구원

4.4 운영 모니터링 및 감사 대응 체계

AI 활용 현황을 상시적으로 식별·관리할 수 있는 운영 가시성 확보 체계 필요

조직 내 AI 활용 현황의 가시성 확보

AI 활용이 확대될수록 자산운용사는 조직 내에서 어떠한 AI가 어떠한 업무에 활용되고 있는지를 지속적으로 파악할 수 있어야 한다. 현업 조직이 다양한 AI 서비스와 자동화 기능을 직접 활용하는 환경에서는 조직 차원에서 실제 AI 활용 현황을 충분히 인지하지 못하는 상황이 발생할 수 있기 때문이다. 따라서 AI 활용 전반에 대한 운영 가시성을 확보하고 이를 관리 범위 안에서 통제할 수 있는 체계를 마련하는 것이 중요하다.

이를 위해 자산운용사는 조직 내에서 운영 중인 AI 기능과 서비스, 자동화 흐름을 체계적으로 식별·관리할 수 있는 관리 체계를 구축할 필요가 있다. 최근에는 생성형 AI 서비스뿐 아니라 API 기반 AI 기능과 자동화 플랫폼을 활용한 업무 자동화 사례 역시 빠르게 증가하고 있으며, 일부 활용은 중앙 관리 체계 밖에서 이루어질 가능성도 존재한다. 이에 따라 조직 차원에서는 운영 중인 AI 기능과 활용 목적, 활용 부서, 활용 데이터 등을 체계적으로 관리할 수 있는 AI 인벤토리(AI Inventory)를 구축할 필요가 있다.

또한 AI 활용 현황은 일회성 점검만으로 관리하기 어렵다는 점도 고려해야 한다. AI 환경에서는 새로운 서비스와 기능이 지속적으로 도입되고 업무 흐름 역시 빠르게 변화할 수 있기 때문이다. 따라서 운영 중인 AI 활용 구조와 자동화 흐름을 상시적으로 점검하고, 신규 활용 사례를 지속적으로 관리 범위 안으로 편입할 수 있는 운영 체계를 함께 마련할 필요가 있다.

AI 운영 로그 및 활용 이력 관리

AI 활용 과정은 운영 로그와 활용 이력을 기반으로 추적 가능하도록 기록·관리되어야 한다. AI가 실제 업무 과정에 활용되는 범위가 확대될수록 어떠한 AI가 사용되었고, 어떠한 검토와 승인 절차를 거쳐 결과가 활용되었는지를 확인할 수 있어야 하기 때문이다. 특히 투자 분석과 고객 관련 업무, 중요 내부통제 업무에서는 AI 활용 과정과 승인 기록, 검토 내역 등을 체계적으로 관리할 필요가 있다.

AI 자동화 환경에서는 데이터 이동과 결과 활용 과정이 복잡해지면서 입력·출력 정보와 AI 활용 과정에서 생성되는 주요 기록의 관리 중요성 역시 높아지고 있다. AI 활용 이력이 적절하게 관리되지 않을 경우 결과가 어떠한 과정을 거쳐 생성·활용되었는지를 확인하기 어려워질 수 있으며, 문제 발생 시 원인 분석과 책임 범위 확인에도 제약이 발생할 수 있다.

따라서 자산운용사는 AI 활용 과정 전반에 대한 운영 로그와 활용 이력을 체계적으로 관리함으로써 결과의 추적 가능성을 확보하고, 내부통제 및 사후 검증의 기반을 마련할 필요가 있다.

감사 대응 및 입증 체계 운영

자산운용사는 실제 AI 운영 과정에서 어떠한 검토와 승인, 통제 활동이 수행되었는지를 사후적으로 설명하고 입증할 수 있어야 한다. AI가 투자 분석과 의사결정 지원, 내부통제 업무 등 다양한 영역에 활용될수록 결과뿐 아니라 해당 결과가 어떠한 기준과 절차 아래 생성되고 검토·활용되었는지를 확인할 수 있어야 하기 때문이다.

특히 금융산업은 투자자 보호와 내부통제 요구 수준이 높은 산업이라는 점에서, AI 활용 역시 감사 및 사후 검증이 가능한 형태로 운영되어야 한다. 이에 따라 자산운용사는 AI 활용과 관련된 주요 의사결정 과정과 승인 내역, 검토 기록, 통제 활동 수행 여부 등을 객관적으로 확인할 수 있는 감사 대응 체계를 구축할 필요가 있다. 더불어 중요 AI 활용 사례에 대해서는 관련 증적과 검토 이력을 체계적으로 보존함으로써 필요 시 활용 과정 전반을 재구성하고 설명할 수 있어야 한다.

4.5 보안 및 접근통제 체계

AI 활용 과정에서 발생할 수 있는 정보 유출과 권한 오남용, AI 특화 위협 등에 대응할 수 있는 보안 및 접근통제 체계 강화 필요

AI 활용이 확대되면서 자산운용사의 보안 관리 범위 역시 기존 IT 시스템 중심에서 AI 활용 환경 전반으로 확대되고 있다. AI는 다양한 데이터와 외부 서비스, 내부 업무 시스템을 연결하는 형태로 활용될 수 있다는 점에서, 기존의 네트워크와 시스템 중심 보안 체계만으로는 충분히 대응하기 어려운 측면이 존재한다. 이에 따라 자산운용사는 AI 활용 과정에서 발생할 수 있는 정보 유출과 권한 오남용, AI 특화 보안 위협 등에 대응할 수 있는 보안 및 접근통제 체계를 보다 강화할 필요가 있다.

정보보호 및 데이터 유출 방지

AI 활용이 확대되면서 자산운용사가 보유한 고객정보와 거래정보, 내부 리서치 자료, 투자전략 정보 등 다양한 중요 정보가 AI 활용 과정에서 처리되는 사례가 증가하며, 조직 내부 정보가 의도하지 않게 외부 환경으로 전송되거나 저장될 가능성 역시 높아지고 있다. 이에 따라 자산운용사는 AI 활용 과정에서 중요 정보가 외부로 유출되거나 비인가 사용자에게 노출되지 않도록 정보보호 체계를 강화할 필요가 있다.

AI 활용 위험도별 보안 · 통제 기준 예시

구분	항목	위험도				
		Low	Medium	High	Very High	Critical
위험도 결정요인	적용 업무	문서 작성, 번역, 회의록 정리 등 생산성 향상 목적의 보조 업무	리서치 자료 작성, 보고서 초안 작성, 시장 정보 분석 등 분석 지원 업무	투자 분석, 종목 발굴, 포트폴리오 검토 등 투자 판단에 영향을 미칠 수 있는 업무	고객 응대, 투자권유, 고객 성향 분석 등 고객에게 직접 영향을 미치는 업무	투자 의사결정, 주문 집행, 자동화된 투자 프로세스 등 재무적 영향이 직접 발생하는 업무
	활용 데이터	공시자료, 보도자료, 공개 리서치 등 외부 공개 정보	내부 업무자료, 일반 보고서, 조직 내 공유 자료 등 비민감 내부 정보	내부 리서치 자료, 투자 아이디어, 운용 관련 중요 정보	고객정보, 거래정보, 상담 이력 등 개인정보 및 고객 관련 정보	미공개 투자정보, 핵심 투자전략, 중요 경영정보 등 최고 수준 보호가 필요한 정보
	AI 권한 수준	정보 조회, 검색 및 요약 기능 수행	문서 분석, 정보 분류, 초안 작성 등 분석 지원 기능 수행	분석 결과 생성, 업무 프로세스 지원, 내부 시스템 연계 기능 수행	고객 관련 의사결정 지원 또는 업무 처리 권고 기능 수행	업무 실행, 외부 시스템 연계, 자동화된 업무 수행 또는 의사결정 영향 가능 기능 수행
적용 통제수준	인간 개입 수준	사용자 사후 확인 중심	담당자의 결과 검토 및 적정성 확인 필수	독립적 검증 또는 교차 검토 수행 후 활용	준법 · 리스크 부서 검토를 포함한 강화된 인간 개입 수행	Human-in-the-Loop 기반 최종 검토 및 승인 필수
	승인 수준	별도 승인 없이 활용 가능	팀장 또는 부서 책임자 승인	본부장 또는 관리부서 승인	준법감시인 또는 리스크 책임자 승인	위원회 또는 지정 책임임원의 사전 승인
	기록 관리	활용 로그 및 접속 이력 기록	검토 이력 및 활용 목적 기록	승인 내역, 검증 결과 및 활용 이력 기록	감사 대응이 가능한 수준의 검토 · 승인 기록 유지	전체 의사결정 과정 및 감사 추적(Audit Trail) 정보 보관
	보안 통제	기본 정보보호 정책 및 로그 관리 적용	접근 권한 관리, 입력 정보 제한 및 정기 모니터링 적용	강화된 접근통제, 승인 절차 및 이상행위 탐지 체계 적용	데이터 유출 방지, 권한 오남용 방지 등 고강도 통제 적용	최고 수준의 접근통제, 상시 모니터링 및 예외 대응 체계 운영
	운영 원칙	생산성 향상을 위한 보조도구 활용	인간 검토를 전제로 한 업무 지원 수단으로 활용	AI 결과를 참고자료로 활용하되 단독 활용은 제한	고객 영향이 발생하기 전 충분한 검증 및 통제 수행	AI는 지원도구로만 활용하며 최종 판단과 책임은 인간에게 귀속

자료: 삼일PwC경영연구원

데이터 보호와 접근 권한 관리, AI 특화 보안 통제 체계를 통합 운영함으로써 보안 수준과 통제 체계의 일관성 유지 필요

고객식별정보와 미공개 투자정보, 내부 전략자료 등 중요 정보에 대해서는 정보 중요도에 따른 차등 보호 기준을 적용하고, 외부 AI 서비스 활용 시에는 입력 제한과 마스킹, 암호화 등 적절한 보호 조치를 함께 운영할 필요가 있다.

또한 AI 활용 환경에서는 데이터가 다양한 시스템과 서비스 간에 이동·처리될 수 있다는 점에서 정보 저장과 전송, 활용 전 과정에 걸쳐 일관된 정보보호 기준을 적용할 필요가 있다. 이를 통해 AI 활용 확대 과정에서도 중요 정보의 유출 가능성을 최소화하고, 조직의 정보보호 수준이 안정적으로 유지될 수 있도록 관리할 필요가 있다.

접근 권한 및 AI 활동 통제 체계 운영

AI 활용이 확대될수록 데이터와 시스템에 대한 접근 권한 관리의 중요성 역시 더욱 높아지고 있다. AI는 다양한 내부 데이터와 업무 시스템, 외부 서비스와 연계되어 활용될 수 있으며, 활용 범위가 확대될수록 접근 가능한 정보와 수행 가능한 업무 범위 역시 함께 증가할 수 있기 때문이다. 이에 따라 자산운용사는 AI 활용 과정에서 부여되는 권한이 적정한 수준으로 통제되고 있는지를 지속적으로 관리할 필요가 있다.

특히 AI 기반 기능이 업무 지원과 정보 검색, 업무 자동화 등 다양한 영역에서 활용될 경우, 과도한 권한 부여는 중요 정보 노출이나 비인가 업무 수행, 권한 오남용 등의 위험으로 이어질 수 있다. 따라서 자산운용사는 최소권한 원칙(Least Privilege)에 기반하여 사용자와 AI 기능에 부여되는 권한 범위를 업무 목적에 필요한 수준으로 제한하고, 중요 데이터와 핵심 업무 기능에 대해서는 추가 승인 절차나 차등화된 접근통제를 적용할 필요가 있다.

또한 접근 권한 관리가 단순한 권한 부여에 그쳐서는 안 되며, 실제 권한 사용 현황에 대한 지속적인 모니터링과 점검 체계가 함께 운영될 필요가 있다. 이에 따라 주요 데이터 접근 이력과 권한 사용 내역, 중요 업무 수행 기록 등을 추적·관리함으로써 권한 오남용과 비인가 접근 가능성을 최소화하고, AI 활용 확대 과정에서도 내부통제 수준이 일관되게 유지될 수 있도록 관리할 필요가 있다.

AI 특화 보안 위협 대응 체계 구축

생성형 AI 환경에서는 기존 보안 체계에서 충분히 고려되지 않았던 새로운 유형의 보안 위협 역시 등장하고 있다. 특히 프롬프트 인젝션(Prompt Injection)과 악성 입력 기반 공격, 외부 콘텐츠를 통한 지시문 변조, 권한 우회 시도 등은 AI 환경에서 새롭게 부상하는 대표적인 보안 위협으로 볼 수 있다.

이에 따라 자산운용사는 외부 문서와 이메일, 웹페이지 등 AI가 처리하는 입력 정보에 대한 검증 절차를 마련하고, 외부 입력과 업무 실행 명령을 분리할 수 있는 통제 체계를 구축할 필요가 있다. 또한 중요 업무와 자동화 기능에 대해서는 사용자 승인 절차와 추가 검증 체계를 함께 운영함으로써 AI 기반 업무 수행 과정에서 발생할 수 있는 보안 위험을 최소화할 필요가 있다.

AI 활용 확대는 보안의 범위를 기존 시스템 보호에서 AI 활용 과정 전반에 대한 통제로 확장시키고 있다. 이에 따라 자산운용사는 데이터 보호와 접근 권한 관리, AI 특화 보안 통제 체계를 통합적으로 운영함으로써 AI 활용 확대 과정에서도 보안 수준과 통제 체계가 일관되게 유지될 수 있도록 관리할 필요가 있다.

4.6 외부 AI 서비스 및 공급망 관리

생성형 AI 등은 복수의 외부 인프라와 연계된다는 점에서 기존 아웃소싱 · 솔루션과는 구분되는 관리 체계 구축 필요

AI 활용 확대와 함께 자산운용사가 활용하는 기술 환경 역시 빠르게 외부화되고 있다. AI 기능은 클라우드와 외부 AI 모델, API, 데이터 서비스 등 다양한 외부 인프라와 연계되어 운영되는 경우가 많기 때문에 기존 IT 아웃소싱이나 솔루션 도입과는 다른 형태의 공급망 · 제3자 리스크가 발생할 수 있다. 이에 외부 AI 서비스 및 공급망 관리 체계 역시 보다 체계적으로 정비될 필요가 있다.

외부 연계 및 신뢰관계 통제 체계 강화

AI 활용이 확대될수록 외부 AI 서비스와 내부 데이터, 업무 시스템 간 연결 역시 증가하게 된다. 특히 외부 AI 서비스는 단순 정보 조회를 넘어 문서 검색과 업무 자동화, API 연계 등 다양한 형태로 활용될 수 있다는 점에서, 외부 서비스가 접근 가능한 데이터와 시스템 범위에 대한 관리 중요성이 높아지고 있다. 또한 정상적인 외부 서비스와 API, SaaS 등을 악용한 공급망 기반 공격 가능성 역시 확대되고 있다는 점에서 외부 연계 구조 전반에 대한 통제 체계를 강화할 필요가 있다.

이에 따라 자산운용사는 외부 AI 서비스와 연결되는 데이터 및 시스템 접근 범위를 최소화하고, 중요 정보와 핵심 업무 기능에 대해서는 추가적인 승인과 통제를 적용할 필요가 있다. 또한 외부 AI 서비스와 API, 플러그인, 자동화 기능 등 외부 연계 요소에 대해서는 사전 검증과 승인 절차를 운영함으로써 비인가 서비스 연계와 신뢰 관계 악용 가능성을 최소화할 필요가 있다.

아울러 외부 서비스와의 연결 구조 및 접근 현황을 지속적으로 점검하고 모니터링함으로써 예상하지 못한 데이터 이동이나 비정상적인 접근 시도를 조기에 식별할 수 있는 관리 체계를 함께 운영할 필요가 있다.

운영 연속성 및 사업자 의존 리스크 관리

AI 활용 확대와 함께 외부 AI 서비스와 클라우드, 데이터 서비스 등에 대한 의존도가 높아지면서 외부 사업자의 장애나 서비스 중단, 정책 변경이 금융회사의 업무 수행에 직접적인 영향을 미칠 가능성이 확대되고 있다. 특히 AI 기반 업무 환경에서는 하나의 외부 서비스가 다수의 업무와 시스템에 연결될 수 있다는 점에서, 단일 사업자 문제 역시 예상보다 광범위한 운영 리스크로 확산될 수 있다. 이에 따라 자산운용사는 외부 AI 서비스 활용 과정에서 발생할 수 있는 사업자 의존 리스크를 관리하고 운영 연속성을 확보하기 위한 체계를 마련할 필요가 있다.

우선 핵심 업무와 연결된 외부 AI 서비스에 대한 의존도를 지속적으로 점검하고, 특정 사업자에 대한 과도한 집중이 발생하지 않도록 관리할 필요가 있다. 이를 위해 대체 서비스 확보와 멀티 벤더(Multi-Vendor) 전략, 서비스 전환 가능성 검토 등을 통해 특정 사업자 장애나 정책 변화가 핵심 업무에 미치는 영향을 최소화할 필요가 있다.

또한 외부 서비스 장애나 예상치 못한 서비스 중단 상황에 대비한 비상 대응 체계를 사전에 마련할 필요가 있다. AI 서비스 이용이 제한되거나 업무 수행에 필요한 기능을 제공받지 못하는 경우에도 핵심 업무가 지속될 수 있도록 수동 업무 전환 절차와 비상 운영 프로세스, 보고 체계 등을 명확히 정의하고 정기적으로 점검할 필요가 있다. 이를 통해 외부 사업자 이슈가 발생하더라도 업무 연속성과 운영 안정성을 유지할 수 있도록 관리해야 한다.

외부 서비스와의 신뢰 관계 악용 가능성에 대비한 공급망 보안 통제 체계 강화 필요

외부 연계 환경의 공급망 보안 통제 체계 강화

AI 활용 확대와 함께 외부 AI 서비스와 API, SaaS, 업무 자동화 플랫폼 등 다양한 외부 서비스가 내부 시스템과 직접 연결되는 사례가 증가하고 있다. 이 과정에서 AI 서비스와 연계된 외부 플러그인이나 자동화 기능이 외부 공격자나 악의적 행위자에 의해 침해될 경우, 해당 기능은 정상 서비스로 인식된 상태에서 내부 시스템과 데이터에 접근할 수 있다. 예를 들어 공격자가 외부 플러그인 제공사의 계정을 탈취하거나 업데이트 서버를 침해할 경우, 악성 코드가 정상 업데이트 형태로 배포될 수 있으며, 사용자는 이를 인지하지 못한 채 내부 문서나 업무 데이터를 외부로 전송하게 될 가능성이 존재한다.

이에 따라 자산운용사는 외부 서비스와의 연결 구조 및 신뢰 관계를 관리할 수 있는 공급망 보안 체계를 강화할 필요가 있다. 공급망 기반 보안 위협은 외부 서비스 자체에 대한 공격뿐 아니라 정상적인 서비스와의 신뢰 관계를 악용하는 방식으로 발생할 수 있다는 점에서, 단순히 개별 서비스의 보안 수준을 점검하는 것만으로는 충분한 대응이 어려울 수 있기 때문이다.

이를 위해 외부 AI 서비스와 API, 플러그인, 자동화 기능 등 외부 연계 요소에 대해서는 사전 검증과 승인 절차를 운영하고, 신뢰할 수 있는 서비스만 활용할 수 있도록 관리할 필요가 있다. 또한 외부 서비스에 부여되는 접근 권한과 데이터 활용 범위를 최소화함으로써 외부 서비스가 침해되거나 악용되더라도 영향 범위를 제한할 수 있도록 관리할 필요가 있다.

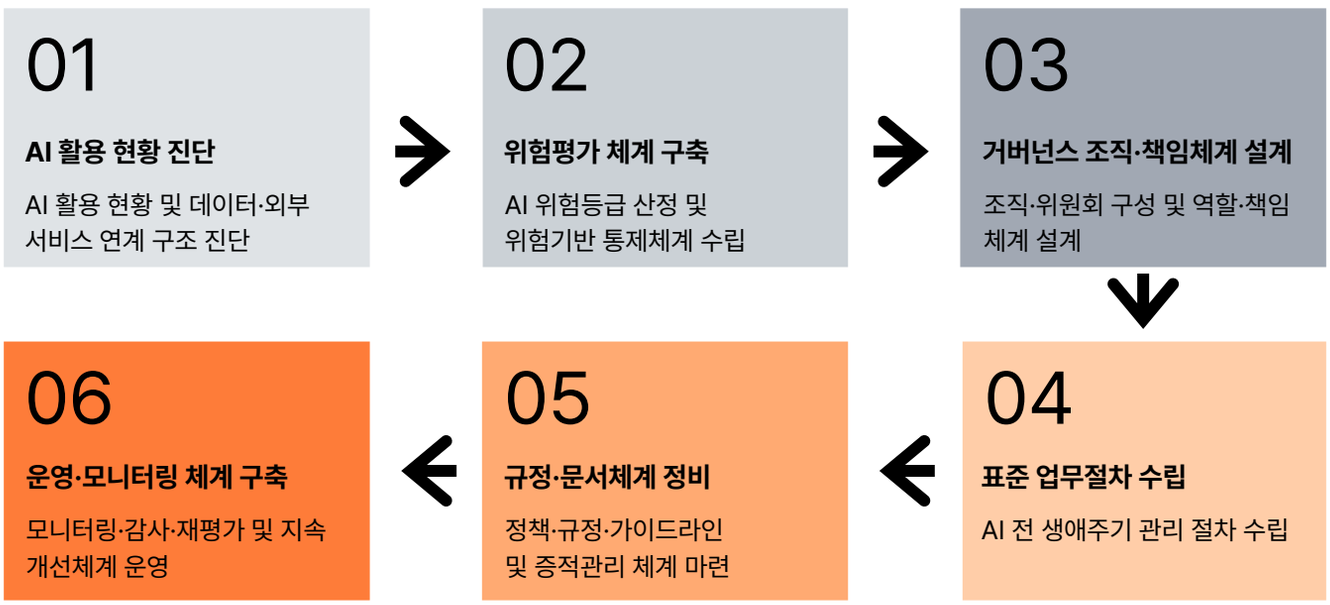
아울러 공급망 기반 공격은 정상적인 서비스 이용 과정에서 발생할 수 있다는 점에서 지속적인 모니터링과 이상행위 탐지 체계를 함께 운영할 필요가 있다. 외부 서비스와의 연결 현황 및 접근 활동을 상시 점검하고, 비정상적인 데이터 이동이나 예상하지 못한 서비스 연계가 발생할 경우 이를 신속하게 식별·대응할 수 있는 관리 체계를 구축함으로써 공급망 기반 보안 위협에 대한 대응 역량을 강화할 필요가 있다.

삼일PwC AI 거버넌스

삼일PwC는 자본시장법·지배구조법·책무구조도 자문 경험과 금융분야 AI 위험관리 프레임워크 적용 역량을 바탕으로, 금융회사의 규모와 AI 활용 수준에 적합한 맞춤형 AI 거버넌스 및 위험관리 체계 구축을 지원합니다.

Samil PwC | AI 거버넌스 전문팀

대형 자산운용사뿐 아니라 중소형 자산운용사도 규모와 운영 환경에 적합한 AI 거버넌스 조직·절차·규정 체계를 구축하고, 실제 업무 운영과 내부통제에 적용 가능한 실효성 있는 관리체계 구현 지원



Business Contact

Leadership

이승환 Partner
AX Node, Leader
seung-whan.lee@pwc.com

김경구 Partner
금융산업, Leader
kyoungkoo.kim@pwc.com

전용욱 Partner
AX Node, Deputy Leader
yong-wook.jun@pwc.com

Primary Contact

정해민 Partner
AX Node, AWM Sector Leader
hai-min.jeong@pwc.com

이종연 Director
AX Node, AWM Specialist
jongyeon.lee@pwc.com

변지현 Director
FS, AWM Specialist
ji-hyun.byun@pwc.com

심교연 Sr. Manager
AX Node, AWM Specialist
kyo-yeon.sim@pwc.com

조여진 Sr. Manager
FS, AWM Specialist
yeojin.cho@pwc.com

Author Contacts

곽호경 수석연구위원

삼일PwC경영연구원
hokyung.kwak@pwc.com

삼일PwC경영연구원

최재영 경영연구원장

jaeyoung.j.choi@pwc.com

삼일회계법인

S/N: 2606W-RP-078