pwc 삼일회계법인

책임 있는(Responsible) AI

AI가 비즈니스의 일부가 된 지금,
외부감사는 무엇을 의미하는가

요약

- 비즈니스 기능 전반에 걸쳐 AI 도입이 가속화됨에 따라 많은 기업들이 변화하는 감사 기대치에 맞추어 AI 활용 방식을 조정하는 방법을 지속적으로 모색하고 있습니다.
- 감사인은 특히 SOX 관련 프로세스나 재무 보고에 AI가 사용될 때, AI의 거버넌스, 문서화 및 통제 방식을 평가할 수 있습니다.
- 강력한 거버넌스 및 위험 분류를 통해 AI 사용에 대한 명확한 가시성을 확보하면 조직이 복잡성을 관리하고 감사 준비 상태를 유지하는 데 도움이 됩니다.
- 검증, 모니터링 및 문서화를 통해 AI 결과물의 신뢰성을 입증하는 것은 감사인 및 이해관계자들과 자신 있게 소통하는 데 필수적입니다.

서론

AI는 비즈니스 수행 방식을 재편하고 있습니다. 귀사 역시 예외가 아닙니다.

재무, 내부 감사부터 IT 및 연구개발에 이르기까지, 귀사는 이미 AI를 활용하여 더욱 빠르고 심층적인 분석을 통해 더 많은 업무를 처리하고 있습니다. 그리고 이는 귀사만의 이야기가 아닙니다. 고객, 서비스 제공업체, 통제 및 규정 준수를 평가하는 팀 등 여러 이해관계자들 모두 AI를 통해 진화하고 있습니다.

이에 따라 중요한 질문이 제기됩니다:

그렇다면 AI 활용이 확대되는 상황에서, 신뢰와 검증(Assurance)은 어떤 의미를 갖게 될 것인가

최고재무관리자(CFO)는 AI가 재무보고에 대한 내부통제(ICFR)에 어떤 변화를 가져올지 궁금해할 수 있습니다. 감사위원회는 자신들의 감독 기능이 변화의 속도를 따라가고 있는지 의문을 가질 수 있습니다. 내부감사팀은 AI 기반 프로세스를 평가할 때 감사인이 어떠한 새로운 데이터, 문서 또는 증거를 요구할지 이해하고자 할 것입니다.

이 모든 것을 파악하는 것은 쉽지 않으며 명확한 기준이 부족하다는 점에서 더욱 복잡합니다. 그러나 한 가지는 분명합니다: AI가 귀사의 프로세스 일부라면, 감사 대상에도 포함된다는 것입니다.

감사인이 어떤 사항을 요구하는지, 그리고 그 요구가 갖는 의미

감사에 대비하는 것이 AI 개발 노력을 늦춘다는 의미는 아닙니다.그러나 Responsible AI 관행에 지속적으로 집중해야 합니다. AI가 의사결정, 고객 상호작용 또는 내부 운영을 지원하든, 조직은 AI의 사용 방식을 설명하고 어떻게 거버넌스, 문서화 및 통제가 이루어지는지 보여줄 준비가 되어 있어야 합니다. 이는 감사인 및 이해관계자들과 신뢰를 구축하는 데 매우 중요한 요소입니다.

감사인은 하향식(top-down) 접근 방식을 통하여 조직이 AI 위험을 관리하고 새로운 시스템 및 기능을 감독하는 방식을 명확히 설명하는 정책, 절차 및 프레임워크를 검토할 수 있습니다. 여기에는 새로운 AI 위험에 대한 대응 방식, 위험 허용 범위 정의, 예외 사항의 보고 절차 등이 포함될 수 있습니다. AI 책임과 관련된 역할과 책임도 검토 대상이 될 수 있습니다. 이러한 영역은 일반적으로 위험 및 통제 프레임워크 또는 이와 유사한 방법론을 통해 평가 및 문서화됩니다. 또한 주요 통제가 효과적으로 운영되었음을 입증하는 문서를 제출하도록 요구 받을 수 있습니다.

예를 들어, 프레임워크에서 배포 전에 모델 위험 평가를 요구하는 경우, 감사인은 해당 요구사항이 존재하는지 뿐만 아니라 실제로 준수되었는지도 확인할 수 있습니다. 여기에는 모델 문서화에 대한 검토자 의견, 문제 보고 증거 또는 설명 가능성 및 편향 검토 산출물 등이 포함될 수 있습니다. AI 거버넌스는 전통적인 통제 프레임워크 범위에서 벗어나는 검토 활동들을 도입하는 경우가 많지만, 이러한 활동이 프로그램의 일부인 경우 감사인은 프레임워크가 실제로 어떻게 적용되고 있는지 입증하는 증거를 찾을 수 있습니다.

외부감사 대응을 위한 준비 사항

조직의 AI 도입 단계와 관계없이 감사에 대비한 AI 관행을 구축하기 위한 방법은 다음과 같습니다.

1 강력한 거버넌스를 구축하십시오.

거버넌스는 어떤 모델이나 도구를 사용할지 결정하는 방식, 해당 도구를 지속적으로 모니터링하는 방법, 그리고 설명 가능성과 데이터 출처를 다루는 방법을 포함해야 합니다. 이는 특히 결과물이 재무 보고나 외부 공시에 활용될 때 더욱 중요합니다. 내부 감사는 새로운 위험을 평가하고, 통제 설계의 타당성을 검증하며, 거버넌스 관행이 의도한대로 운영되는지 평가하는 데 핵심적인 역할을 수행할 수 있습니다. AI 관련 위험은 기존 위험 관리 역량에 통합되어야 합니다. 여기에는 기업 위험 분류체계와 위험 및 위험과 통제의 자기평가가 포함됩니다. 이러한 요소들은 조직이 AI가 제기하는 고유한 위험을 이해하고 있으며, 해당 위험을 효과적으로 평가, 모니터링 및 완화하기 위한 프로세스, 도구 및 책임 체계를 갖추고 있음을 입증하는 데 도움이 됩니다.

2 팀의 역량을 강화하고 목표를 일치시키세요.

감사 준비는 회사 담당팀이 AI 사용 및 거버넌스를 설명하고 결과물의 신뢰성 및 정확성을 설명할 수 있는 능력에 달려 있습니다. 프로세스 책임자와 통제 운영자는 감사 관련 대화에 자신 있게 참여할 수 있도록 교육과 배경지식을 갖추어야 하며, AI가 무엇을 하는지, 어떻게 모니터링되는지, 왜 신뢰할 수 있는지 명확하게 설명할 수 있어야 합니다.

3 AI 사용 사례 목록을 작성하세요.

조직은 비즈니스 전반에 걸쳐 AI가 어디에서 사용되고 있는지 명확하게 파악할 준비가 되어 있어야 합니다. 이를 위한 효과적인 방법은 완전하고 정확한 목록을 유지하는 것으로, 사용 사례를 핵심 비즈니스 프로세스와 연결하고 내부통제(SOX) 또는 기타 규제 영역과 관련된 항목을 표시해야 합니다. 핵심은 조직이 프로세스 전반에 걸친 AI 사용과 각 프로세스에 대한 평가된 위험 수준을 명확하게 이해하고 있음을 입증하는 것입니다. 이러한 목록을 작성할 때 단순히 자체 보고에만 의존해서는 안 됩니다.

***섀도우 AI(shadow AI)** 또는 간과되기 쉬운 영역을 식별할 수 있는 프로세스를 함께 구축해야 합니다. 여기에는 **외부 솔루션에 내재된 AI 기능**, **공식 승인 없이 도입된 AI 활용 사례**, 그리고 **시스템 업데이트를 통해 새롭게 추가된 AI 기반 기능** 등이 포함됩니다.

*섀도우 AI(Shadow AI): 조직의 공식 관리·통제 체계 밖에서 활용되는 AI

이는 공식 프로그램 외의 사용 사례를 포함하여 관련 조직 내 모든 관련 AI 활용 사례가 누락 없이 식별되고 관리되고 있음을 확인할 수 있습니다.

중앙 집중식 목록 관리가 모범 사례로 여겨지지만, AI가 어디서 어떻게 사용되는지를 명확하게 보여주는 잘 문서화된 프로세스만으로도 경우에 따라 충분한 가시성을 제공할 수 있습니다. 특히 이는 **SOX 체계 하에서의 경영진 책임**의 일환으로 고려될 수 있습니다. 어떤 접근 방식을 취하든, 조직은 제3자 시스템에 내재되거나 외부 솔루션을 통해 지원되는 AI기능도 포함하여 AI 사용 현황을 명확하게 파악할 수 있어야 합니다. 이러한 가시성은 리스크를 평가하고 향후 감사에 대비하기 위한 필수 요소입니다.

4 리스크 기반 접근 방식을 적용하십시오.

모든 AI가 동일한 리스크를 갖는 것은 아닙니다. 정책, 절차 및 필수 통제를 포함한 거버넌스 접근 방식은 조직 내에서 AI가 사용되는 방식의 차이를 충분히 반영해야 합니다. 이를 위해 AI 활용 사례를 체계적으로 평가할 수 있는 분류 체계를 도입하는 것을 고려할 필요가 있습니다. 구조화된 분류 체계 및 메타데이터 전략은 지속적인 거버넌스 관리를 보다 용이하게 만들 뿐만 아니라, AI 혁신 속도에 발맞춰 신뢰 확보 및 검증 활동이 함께 진화할 수 있도록 돕습니다.

예를 들어 문서 요약과 같은 활용 사례는 AI 에이전트가 재무 보고서나 규제 보고서를 작성하는 자율 의사 결정과 같은 복잡한 AI활용사례보다 상대적으로 낮은 리스크를 가질 가능성이 큽니다. 명확한 분류 체계는 보다 강도 높은 거버넌스 검증이나 추가적인 검토가 필요한 영역을 신속하게 식별하는데 도움을 줍니다.

이러한 접근 방식을 효과적으로 지원하기 위해 각 AI활용 사례에는 업무 기능, 규제 환경, SOX 관련성 및 데이터 민감도와 같은 적절한 메타데이터가 함께 관리되어야 합니다. 이는 단순히 외부감사 대응 준비에 그치지 않고 조직 전반에 걸쳐 **수백 개, 나아가 수천 개의 AI 활용 사례로 확장될 경우 필수적인 관리 기반**이 됩니다.

5 AI 산출물을 검증하세요.

각 AI 활용 사례별로 조직에서 AI 생성 결과물의 신뢰성을 확인하는 방법을 정의해야 합니다. 여기에는 모델 설계에서 발견된 위험을 해결하기 위해 필요한 추가 검토 사항을 식별하는 것도 포함됩니다. 특히 AI가 재무 보고에 사용될 때 결과물 검증은 매우 중요합니다. 조직이 AI 결과에 대해 충분한 신뢰를 확보하고 있음을 입증할 수 있다면 외부 이해관계자(외부 감사인을 포함한)와의 논의 역시 보다 원활하게 진행될 수 있습니다.

외부 감사 목적으로 AI 결과를 검증한다는 것은 결과가 신뢰할 수 있고, 적절히 검토되었으며, 거버넌스 체계 하에서 관리되고 있음을 보여주는 증빙을 제시할 수 있어야 함을 의미합니다. 다음은 외부 감사 준비 상태를 입증하는 데 도움이 될 수 있는 몇 가지 예시 자료입니다.

- 모델 리스크 평가 또는 검증 승인
- 검토 코멘트 또는 승인 업무흐름
- 예외 기록 및 이슈 보고 문서
- 사람의 검토가 이루어졌음을 보여주는 산출물 샘플모니터링 보고서(예: 드리프트 감지, 알림 임계값)

AI 판단을 대체하거나 무효화한 통제 조치 및 승인 내역에 대한 문서화AI 활용 프로세스를 반영하여 업데이트된 SOX 문서검토 단계와 결과, 대체 메커니즘 및 기대 성과 수준을 명확하게 정의하고 문서화해야 합니다. 많은 AI 시스템은 결정론적(deterministic) 결과가 아니라 확률론적(probabilistic) 결과를 생성한다는 점(즉, 고정된 규칙이 아닌 가능성에 기반한 결과) 에서 외부 감사인은 이러한 특성으로 인한 리스크를 조직이 어떻게 관리하고 있는지에 대해 관심을 가질 가능성이 큽니다. 여기에는 AI가 기존 프로세스나 통제 단계를 보완하거나 대체하는 경우, 테스트 및 검토 요건이 어떻게 정의되고 적용되는지도 포함됩니다.

특히 **생성형 AI가 재무 성과를 요약하거나 공시용 서술 정보를 작성하는 데 사용되는 경우**, 정확성에 대해 고정된 고정된 임계값을 설정하는 것은 현실적으로 어려울 수 있습니다. 이러한 상황에서 감사인은 **프롬프트가 어떻게 설계되는지**, **산출물이 어떤 방식으로 검토·승인되는지**, 그리고 **환각(hallucination) 리스크가 어떻게 식별되고 모니터링되는지**에 대한 통제 증빙을 중점적으로 확인할 가능성이 큽니다.

SOX 준수를 위한 준비

SOX 적용을 받는 상장회사라면 감사에 대비하는 것이 특히 중요합니다. 다음 사항들에 대해 귀사는 얼마나 준비되어 있습니까?

1	**재무 보고에서 AI가 어디에서 어떻게 사용되는지 명확하게 설명하십시오.**	외부 감사인은 감사 계획 수립 과정 및 감사 전반에 걸쳐 이와 관련하여 질문할 수 있습니다. 자동분개, 추정치, 결산 프로세스 또는 기타 SOX 관련 영역에서 활용되는AI는 인벤토리 상 명확히 식별되어야 하며 자체 SOX 프로그램 내에도 적절히 고려되어야 합니다.
2	**AI 결과물이 어떻게 검증되는지 입증하십시오.**	데이터 무결성 검사, 검토 단계 및 예외 처리 등 재무제표 및 규제 관련 산출물에 반영되는 AI 생성 결과에 대해 경영진이 어떻게 신뢰를 얻는지 보여줄 수 있어야 합니다.
3	**AI 관련 통제의 설계 및 효과성을 검증하십시오.**	AI 솔루션이 통제의 일부인 경우, 해당 통제가 어떻게 설계되었고, 어떻게 일관되게 운영되는지, 그리고 경영진이 어떻게 검증했는지 문서화해야 합니다. 또한 AI 시스템 또는 솔루션이 어떻게 개발, 배포 및 검증되었는지 보여줄 준비가 되어 있어야 합니다. 필요한 경우, 통제에 AI가 관여하고 있음을 반영하여 통제기술서(RCM: Risk-Control Matrix)을 업데이트해야 하며, AI가 산출물을 생성하는지, 검토하는지, 또는 보조 역할을 하는지도 명확히 구분되어야 합니다.
4	**SOX관련문서를 준비하십시오.**	RCM, 업무기술서 및 업무흐름도에 AI 활용을 정확히 반영하고 있는지 확인해야 합니다. 이 단계를 간과하면 감사 과정에서 귀하의 팀과 외부 감사인 간의 의견 불일치가 발생할 수 있습니다.
5	**프로세스 책임자의 역량을 강화하십시오.**	주요 재무 보고 프로세스 책임자는 AI가 어떻게 사용되는지, 어떤 문제가 발생할 수 있는지, 그리고 업데이트된 통제 방식을 통해 위험을 어떻게 완화하는지 설명할 수 있어야 합니다.

감사준비에서 확신 있는 대응으로

AI가 자동화, 예측 또는 제3자 솔루션에 내재된 형태로 활용되고 있든 상관없이, 조직은 외부 감사 과정에서 AI 활용 방식을 명확하고 자신 있게 설명할 수 있어야 합니다. 여기에서 말하는 감사 준비 단계란, 외부 감사인과 이해관계자 모두에게 신뢰를 줄 수 있는 거버넌스, 문서화 및 통제 구조를 갖추고 있음을 입증할 수 있는 상태를 의미합니다.

감사 준비는 일회성 작업이 아니라 지속적인 노력입니다. AI 기능이 발전함에 따라 거버넌스 및 입증에 대한 기대치도 함께 높아질 것입니다. 견고한 거버넌스 체계, AI 인벤토리 및 산출물 검증 체계를 구축해두면, 감사인이 어려운 질문을 제기할 때 조직은 자신 있게 답변할 수 있을 뿐만 아니라 AI가 기업 전반에 걸쳐 얼마나 책임감 있고 효과적으로 활용되고 있는지 명확하게 설명할 수 있을 것입니다.

Contacts

AX Node

이승환 Partner
AX Node Leader

02-3781-9863
seung-whan.lee@pwc.com

정수정 Partner

02-709-7038
soo.jung.jeong@pwc.com

Unicorn Platform

이도신 Partner
유니콘지원센터센터장

02-709-3321
do-shin.lee@pwc.com

신종훈 Partner

02-709-0209
jonghoon.shin@pwc.com

김광연 Partner

02-3781-9184
kwang-yeon.kim@pwc.com

이용재 Partner

02-709-0393
yong-jae_1.lee@pwc.com

삼일회계법인

S/N: 2601A-RP-018