

## Artificial Intelligence: An Emerging Oversight Responsibility for Audit Committees?

By Brian Cassidy, Ryan Hittner, and Krista Parsons, Deloitte & Touche LLP

The audit committee has many discrete duties, including overseeing financial reporting and related internal controls, the independent and internal auditors, and ethics and compliance, to name just a few. However, these and other duties are part of a broader audit committee responsibility: risk oversight. While the audit committee does not manage all risks, it is responsible for overseeing the procedures and processes by which the company anticipates, evaluates, monitors, and manages risks of all types. Recent developments in artificial intelligence (AI), including the emergence of generative AI, are leading businesses to evaluate AI's potential impact to their business technology strategy. As businesses expand their use of AI, especially into core business processes, the audit committee will need to understand the challenges and opportunities presented by AI to address risks related to governance and stakeholder trust.

### WHO'S MINDING THE AI STORE NOW?

According to a 2023 survey conducted by Deloitte and the Society for Corporate Governance, corporate secretaries see AI strategy and oversight as still evolving. The findings show that few respondents (13%) had a formalized AI oversight framework, although many (36%) were considering the development and implementation of AI oversight policies and procedures.

## 인공지능(AI) : 감사위원회의 새로운 감독 영역인가?

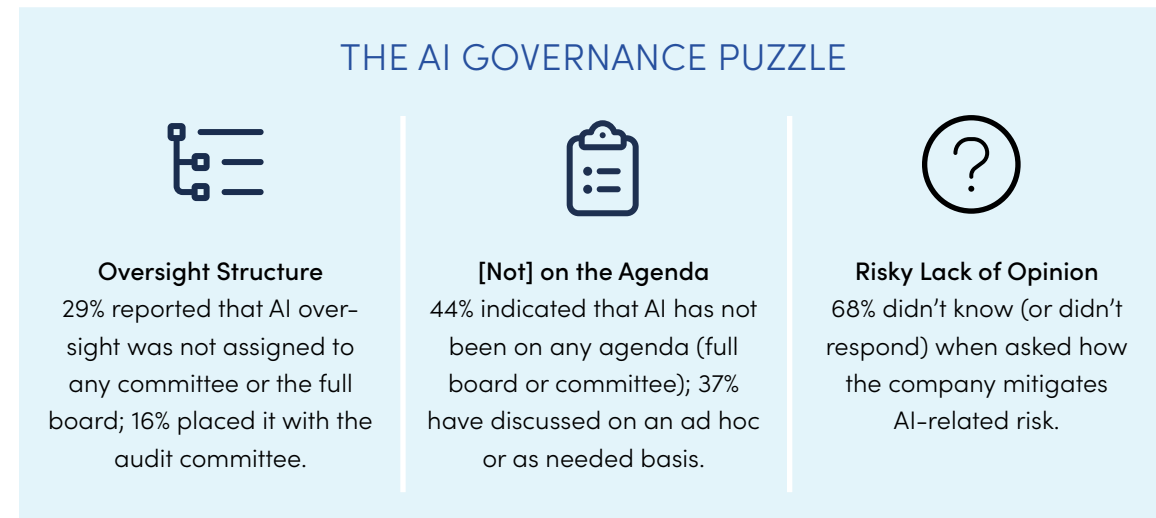
감사위원회는 재무보고 및 관련 내부통제, 독립 및 내부감사인, 윤리 및 컴플라이언스를 감독하는 등 여러가지 개별적 업무를 수행합니다. 그러나, 이러한 업무와 기타 업무는 리스크 감독이라는 감사위원회의 보다 광범위한 책임 중 일부입니다. 감사위원회는 모든 리스크를 관리하는 것은 아니지만, 회사가 모든 유형의 리스크를 예측, 평가, 모니터링 및 관리하는 절차와 프로세스를 감독할 책임이 있습니다. 최근 생성형 AI의 출현을 비롯한 인공지능(AI)의 발전으로 인해 기업들은 비즈니스 기술 전략에 대한 AI의 잠재적 영향을 평가하고 있습니다. 기업이 특히 핵심 비즈니스 프로세스에 AI 사용을 확대함에 따라 감사위원회는 거버넌스 및 이해관계자 신뢰와 관련된 리스크를 해결하기 위해 AI가 제시하는 도전과 기회를 이해해야 합니다.

### 지금 누가 AI를 관리하는가?

델로이트와 기업 거버넌스 협회(Society for Corporate Governance)가 실시한 2023년 서베이에 따르면, 코퍼레이트 세크리터리(Corporate Secretary)는 AI 전략과 감독이 계속 발전중인 것으로 보고 있습니다. 많은 응답자(36%)가 AI 감독 규정 및 절차의 개발 및 실행을 고려하고 있지만, 공식화된 AI 감독 프레임워크를 갖추었다고 답변한 응답자(13%)는 거의 없는 것으로 나타났습니다.

\* 코퍼레이트 세크리터리(Corporate Secretary): 미국, 영국 등의 기업에서 기업 법무 및 주주관계 업무를 총괄하는 고위직

These results are particularly interesting when compared to a 2022 Deloitte [survey](#), in which 94 percent of respondents said AI was critical to their company's short-term success.<sup>1</sup> This may suggest some level of information asymmetry between management and the board, congruent with the notion that AI is in a state of flux. Thus, at least for now, the AI landscape might best be characterized as an abstract governance puzzle.<sup>2</sup>



## RISKS AND OPPORTUNITIES

### FAMILIAR AND DIFFERENT SET OF RISKS

With new technology comes the possibility of new risks. Some AI risks present well-trodden challenges that arise in other technology areas and can be overseen and understood in the context of an ongoing enterprise risk management (ERM) process,<sup>3</sup> such as the [COSO ERM framework](#). However, other risks may be unfamiliar and/or amplified. A few illustrative examples are highlighted below.

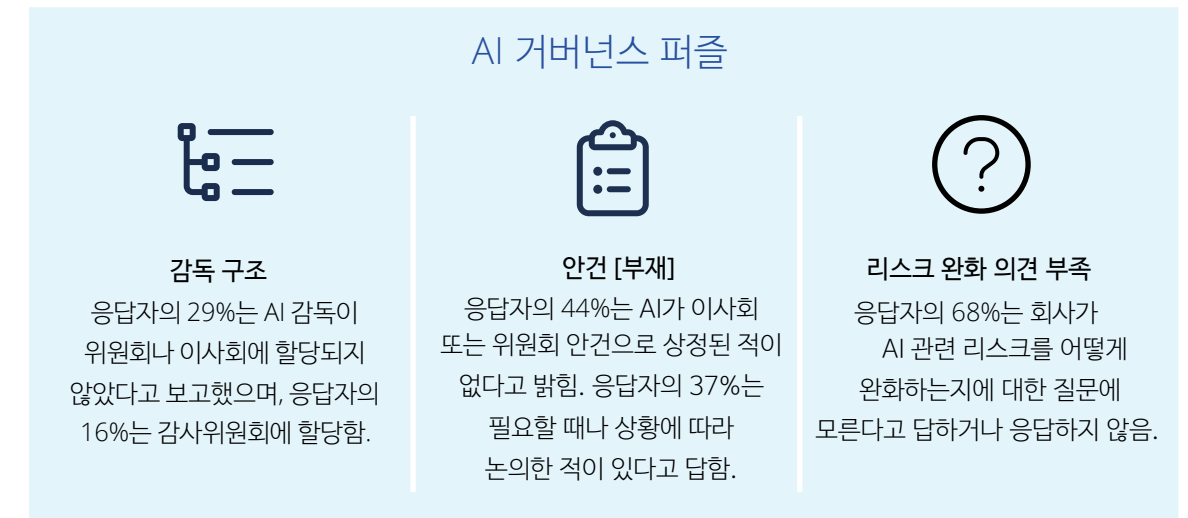
- ▶ **Shadow IT Environments:** Use of IT assets by personnel without the knowledge or oversight of IT security professionals can occur with any type of software or hardware. However, unauthorized use of generative AI by personnel may compound data-related risks. This risk may be increased given the [lack of AI policy](#) in many organizations. Further, employees leveraging generative AI to write code may [inadvertently introduce vulnerabilities](#) through code generated by AI.

<sup>1</sup> Business leaders were defined as company representatives who met one or more of the following qualifiers: (1) responsible for AI technology spending or approval of AI investments, (2) responsible for the development of AI strategy, (3) responsible for implementation of AI technology, (4) acting as AI technology subject-matter specialist, or (5) otherwise stated they were influencing decisions around AI technology. See Nitin Mittal, Irfan Saif, and Beena Ammanath, *Fueling the AI transformation: Four key actions powering widespread value from AI, right now*, *State of AI in the Enterprise, 5th Edition* report, Deloitte, October 2022.

<sup>2</sup> Natalie Cooper, Bob Lamm, and Randi Val Morrison, "Future of tech: Artificial intelligence (AI)," *Board Practices Quarterly*, Deloitte, August 2023.

<sup>3</sup> Alexander J. Wulf and Ognyan Seizov, "Please understand we cannot provide further information': Evaluating content and transparency of GDPR-mandated AI disclosures," *AI & Society* (2022).

이러한 결과는 응답자의 94%가 AI가 회사의 단기적 성공에 중요하다고 답한 2022년 딜로이트 [서베이](#) 결과와 비교하면 특히 흥미롭습니다.<sup>1</sup> 이는 경영진과 이사회 간의 정보 비대칭성이 있음을 시사하며, AI가 유동적인 상태에 있음을 보여줍니다. 따라서 적어도 현재로서는 AI 환경은 추상적인 거버넌스 퍼즐이라고 표현할 수 있습니다.<sup>2</sup>



## 리스크와 기회

### 익숙하면서도 다른 리크스





새로운 기술에는 새로운 리스크가 수반됩니다. 일부 AI 리스크는 다른 기술 영역에서 발생하는 익숙한 도전과제를 제시하며, 이는 [COSO ERM 프레임워크](#)와 같은 지속적인 전사적 리스크 관리 프로세스의 맥락에서 감독하고 이해될 수 있습니다.<sup>3</sup> 그러나 다른 리스크는 생소하거나 확대될 수 있습니다. 아래에 몇 가지 예시가 있습니다.

- ▶ **그림자 IT(Shadow IT) 환경:** IT 보안 전문가의 지식이나 감독 없이 직원이 IT 자산을 사용하는 것은 모든 유형의 소프트웨어 또는 하드웨어에서 발생할 수 있습니다. 그러나, 직원이 생성형 AI를 무단으로 사용하면 데이터 관련 리스크가 더욱 커질 수 있습니다. 많은 조직에서 [AI 규정이 부재한 상황에서 이러한 리스크는 더욱 커질 수 있습니다](#). 또한, 직원이 생성형 AI를 활용하여 코드를 작성할 경우, AI가 생성한 코드를 통해 [의도치 않게 취약점이 노출될 수 있습니다](#).

- ▶ **IP Ownership and Infringement:** Generative AI users can input confidential or protected data, which may result in an array of adverse outcomes, including disclosure of such confidential or protected data to third parties. Outputs using this type of data may also constitute infringement of intellectual property.<sup>4</sup> Furthermore, as generative AI applications are used to craft increasingly sophisticated media across multiple formats, it may not be clear who owns the rights to any resulting intellectual property.
- ▶ **Cybersecurity Bad Actors:** A frequent concern across many types of technology stems from malicious actors who circumvent security protocols. Generative AI use cases may amplify some types of cybersecurity risks. For example, hackers may use generative AI to write code for purposes of infiltrating data environments or create phishing messages that more accurately mimic human language and tone.

Finding the appropriate balance between AI's benefits and risks depends on a constellation of factors. Outputs produced by generative AI change over time as the technology learns from data. But just like with humans, it is possible for this subcategory of AI technology to learn things that are incorrect. For that reason, traditional risk management strategies **may not be well-equipped** for the challenges that arise from generative AI use.

### GENERATIVE AI RISK EXAMPLES

			
<p><b>Low Transparency</b> How generative AI derives its output can be a "black box," making it difficult to explain and/or audit.</p>	<p><b>Hallucination</b> Generative AI products and services may generate output that seems accurate but is actually false or cannot be justified.</p>	<p><b>Bias Potential</b> When trained on nonrepresentative data, generative AI output could exhibit systematic errors.</p>	<p><b>Value Alignment</b> Even with safeguards, generative AI output may contradict its intended purpose.<sup>5</sup></p>

<sup>4</sup> Christian Heinze, "Patent infringement by development and use of artificial intelligence systems, specifically artificial neural networks," in *A Critical Mind: Hanns Ullrich's Footprint in Internal Market Law, Antitrust and Intellectual Property*, eds. Christine Godt and Matthias Lamping, MPI Studies on Intellectual Property and Competition Law, vol. 30 (Heidelberg, Germany: Springer, 2023), pp. 489–515.

<sup>5</sup> Vic Katal, Cory Liepold, and Satish Iyengar, "Artificial intelligence and ethics: An emerging area of board oversight responsibility," *On the Board's Agenda*, Deloitte, 2020.

- ▶ **IP 소유권 및 침해:** 생성형 AI 사용자는 기밀 또는 보호된 데이터를 입력할 수 있으며, 이는 기밀 또는 보호된 데이터가 제3자에게 공개되는 등 다양한 부정적인 결과를 초래할 수 있습니다. 이러한 유형의 데이터를 사용한 결과물은 지적 재산권 침해에 해당할 수 있습니다.<sup>4</sup> 또한, 생성형 AI 애플리케이션이 다양한 형식의 미디어를 더욱 정교하게 제작하는 데 사용되는 경우, 결과물에 대한 지적 재산권의 소유자가 누구인지 명확하지 않을 수 있습니다.
- ▶ **사이버 보안의 악의적 행위자(Bad Actors):** 다양한 기술 분야에서 빈번하게 나타나는 우려는 보안 프로토콜을 우회하는 악의적인 공격자들로부터 비롯됩니다. 생성형 AI 사용 사례는 일부 유형의 사이버보안 리스크를 더 크게 부각시킬 수 있습니다. 예를 들어, 해커는 생성형 AI를 사용하여 데이터 환경에 침투하거나 사람의 언어와 어조를 더 정확하게 모방한 피싱 메시지를 생성하는 등의 목적으로 코드를 작성할 수 있습니다.

AI의 이점과 리스크 사이에서 적절한 균형을 찾는 것은 여러 요인에 따라 달라집니다. 생성형 AI가 데이터로부터 학습하면서 생성하는 결과물은 시간이 지남에 따라 변화합니다. 그러나 인간과 마찬가지로 이 하위 범주의 AI 기술이 잘못된 정보를 학습할 수 있습니다. 따라서 기존의 리스크 관리 전략은 생성형 AI 사용으로 인해 발생하는 문제에 **적절히 대응하지 못할 수 있습니다**.

### 생성형 AI 리스크 사례





			
<p><b>낮은 투명성</b> 생성형 AI가 결과물을 도출하는 방식은 "블랙박스"가 되어 설명하거나 감사하기 어려울 수 있음.</p>	<p><b>환각</b> 생성형 AI 제품 및 서비스는 정확해보이지만 실제로는 거짓이거나 정당화 할 수 없는 결과물을 생성할 수 있음.</p>	<p><b>편향 가능성</b> 대표성이 없는 데이터로 학습할 경우, 생성형 AI의 결과물은 체계적인 오류를 보일 수 있음.</p>	<p><b>가치 정렬</b> 안정장치가 있더라도 생성형 AI의 결과물은 의도한 목적과 상반될 수 있음.<sup>5</sup></p>

Regardless of whether the risk is familiar, completely new, and/or amplified, the resultant consequences may be notable. Failure to mitigate any subcategory of AI-related risks may lead to many adverse outcomes such as reputational damage, financial losses, legal action, and regulatory infractions. A starting point for addressing such concerns might include using mitigation strategies that are already known to work in other contexts, such as the [COSO ERM framework](#) referred to earlier. For AI-centric guidance related to implementation and scaling, it may be worth considering the benefit of systems such as the [NIST AI Risk Management Framework](#).

### WITH RISKS COME BENEFITS, TOO

If AI presented nothing but risk, it seems unlikely that it would have emerged as “the” technology of the future. Clearly, AI has benefits, some of which may not be known for some time. One particular set of benefits is squarely in the audit committee’s wheelhouse—namely, the potential to streamline and enhance a company’s internal audit, financial reporting, and internal control functions. There are also aspects of generative AI technology that, while still evolving, may one day fundamentally change an organization’s financial systems. While there is much uncertainty, the future transformative potential of generative AI may add much to the current array of use cases. In the shorter term, various subcategories of AI are already capable of improving the quality of financial reporting via reviewing transactions, identifying errors, addressing internal control gaps, and detecting fraud. If AI isn’t being used within these areas, the audit committee might ask if the company is exploring potential use cases—and if the company is not, the committee might ask to hear the reasons behind that decision.

#### USE OF AI TECHNOLOGY MAY HAVE MANY BENEFITS





 <p><b>Cost Savings</b> Process automations and improvements may improve task efficiency.</p>	 <p><b>Boosted Revenues</b> AI-infused products and services may provide new growth opportunities.</p>	 <p><b>Development Time</b> AI may shorten time to market by increasing the speed of early-stage testing.</p>	 <p><b>New Insights</b> Appropriate generative AI use may bolster employee creativity.</p>
--	---	--	---

리스크가 친숙한지, 완전히 새로운지, 증폭되었는지에 관계없이 그로 인한 결과는 심각할 수 있습니다. AI 관련 리스크의 하위 범주를 완화하지 못하면 평판 손상, 재정적 손실, 법적 조치, 규제 위반 등 여러가지 부정적인 결과로 이어질 수 있습니다. 이러한 우려를 해결하기 위한 출발점에는 앞서 언급한 [COSO ERM 프레임워크](#)와 같이 다른 상황에서 이미 효과가 있는 것으로 알려진 완화 전략을 사용하는 것일 수 있습니다. 실행 및 확장과 관련된 AI 중심 지침의 경우 국립표준기술연구소(NIST)의 AI 리스크 관리 프레임워크와 같은 시스템의 이점을 고려할 수 있습니다.





### 리스크에 따르는 이점

AI가 리스크만 가지고 있다면 미래의 “기술”로 부상하지 못했을 것입니다. AI에는 분명 이점이 있으며, 그 중 일부는 아직 알려지지 않았을 수도 있습니다. 특히 감사위원회의 핵심 역할인 기업의 내부감사, 재무보고, 내부통제 기능을 간소화하고 강화할 수 있는 잠재력이 바로 그것입니다. 또한, 생성형 AI 기술에는 아직 발전 중이지만 언젠가는 조직의 재무 시스템을 근본적으로 바꿀 수 있는 측면도 있습니다. 많은 불확실성이 존재하지만, 생성형 AI의 미래 혁신적 잠재력은 현재의 다양한 사용 사례에 많은 것을 기여할 수 있습니다. 단기적으로는 이미 다양한 하위 범주의 AI가 거래 검토, 오류 식별, 내부통제 격차 해소, 부정적발을 통해 재무보고의 품질을 개선할 수 있습니다. 이러한 영역에서 AI가 사용되지 않는다면 감사위원회는 회사가 잠재적인 사용 사례를 모색하고 있는지 묻고, 그렇지 않다면 그 결정의 이유를 들어볼 수 있습니다.

#### AI 기술을 사용하면 많은 이점을 얻을 수 있습니다

 <p><b>비용절감</b> 프로세스 자동화 및 개선으로 업무 효율성이 향상될 수 있음.</p>	 <p><b>매출 증대</b> AI가 접목된 제품과 서비스는 새로운 성장 기회를 제공할 수 있음.</p>	 <p><b>개발 시간</b> AI는 초기단계의 테스트 속도를 높여 시장 출시 시간을 단축할 수 있음.</p>	 <p><b>새로운 통찰력</b> 생성형 AI를 적절히 활용하면 직원의 창의성을 강화할 수 있음.</p>
--	---	--	---

## COMMON AI USE CASE EXAMPLES





USE CASE	DESCRIPTION	OPPORTUNITIES	RISKS
 <p><b>Invoices and Payments</b></p>	Use of intelligent automation to match invoices to payments, including classification of expenses	The technology may reduce costs by processing a large volume of transactions with a high degree of accuracy.	Poorly designed or maintained systems may generate errors that are time consuming to undo.
 <p><b>Contract Review or Generation</b></p>	Leverage of natural language and generative AI processing to create legal documents or review them for errors	By producing the initial drafts or identifying common errors, generative AI may create efficiencies and lower legal liability in a cost-effective manner.	Natural language and generative AI trained on <b>biased data</b> may misapply the law or make up precedent.
 <p><b>Forecasting and Modeling</b></p>	Incorporating predictive analytics to improve the accuracy of functions like inventory management and revenue forecasting	Modeling and analytics AI technology may be capable of identifying patterns at a speed that outpaces human-led data analysis efforts.	Lack of robust testing and regular updates can cause modeling and analytics AI to become more inaccurate over time.
 <p><b>Code Development</b></p>	Use of generative AI to develop models or applications that create efficiencies for routine personnel activities	Employees may use generative AI to drive efficiencies in day-to-day tasks and help identify possible generative AI use cases.	The technology may expose confidential data with generative AI inputs or may create outputs that involve intellectual property infringement.

## AI AND THE AUDIT COMMITTEE

The tendency to assign oversight of emerging risks to the audit committee means it is sometimes described as the “kitchen sink” of the board. However, as noted earlier, this is consistent with the audit committee’s overarching role in risk oversight. It’s also worth considering that it is common for topics taken on by the audit committee at the outset to eventually be overseen by other committees. Some aspects of AI oversight seem more aligned with the audit committee’s work than others. And when it comes to considering such congruence questions, it may be helpful to think about the audit committee’s current levels of technology fluency and comfort. For instance, given the audit committee’s traditional governance areas, it may be prudent for it to oversee AI use in financial reporting.<sup>6</sup>

<sup>6</sup> The audit committee may want to also think about indirect impacts. Depending on the use case, AI technology may have an array of indirect effects on financial measures (GAAP or otherwise).

## 일반적인 AI 사용 사례 예시

사용사례	설명	기회	리스크
 <p><b>송장 및 결제</b></p>	지능형 자동화를 사용하여 비용 분류를 포함한 송장과 결제를 일치시킴	이 기술은 높은 정확도로 대량의 거래를 처리함으로써 비용을 절감할 수 있음.	시스템을 잘못 설계하거나 유지 관리하면 오류를 복구하는 데 많은 시간이 소요될 수 있음.
 <p><b>계약서 검토 또는 생성</b></p>	자연어 및 생성형 AI 프로세스 활용을 통해 법률 문서를 작성하거나 오류 검토	생성형 AI는 초안을 작성하거나 일반적인 오류를 식별함으로써 비용 효율적인 방식으로 효율을 높이고 법적 책임을 줄일 수 있음.	<b>편향된 데이터로 학습된</b> 자연어와 생성형 AI는 법을 잘못 적용하거나 판례를 남길 수 있습니다.
 <p><b>예측 및 모델링</b></p>	예측 분석을 통합하여 재고 관리 및 수익 예측과 같은 기능의 정확성 향상	모델링 및 분석 AI 기술은 인간이 주도하는 데이터 분석 작업보다 빠른 속도로 패턴을 식별할 수 있음.	강력한 테스트와 정기적인 업데이트가 부족하면 시간이 지남에 따라 모델링 및 분석 AI의 정확도가 떨어질 수 있음.
 <p><b>코드 개발</b></p>	생성형 AI를 활용하여 일상적인 업무 활동의 효율성을 높이는 모델 또는 어플리케이션 개발	직원은 생성형 AI를 사용하여 일상 업무의 효율성을 높이고 활용 가능한 생성형 AI 사용 사례를 식별하는 데 도움 받을 수 있음.	이 기술은 생성형 AI 입력으로 기밀 데이터를 노출하거나 지적재산권 침해와 관련된 결과물을 생성할 수 있음.

## AI와 감사위원회

새로운 리스크에 대한 감독 책임을 감사위원회에 부여하는 경향이 있기 때문에 감사위원회는 이사회의 “모든 문제를 해결하는 곳”으로 비유하기도 합니다. 그러나 앞서 언급한 바와 같이 이는 리스크 감독에 있어서 감사위원회의 가장 중요한 역할과 일치합니다. 또한, 감사위원회에서 다룬 주제가 결국 다른 위원회에서 감독하는 것이 일반적이라는 점도 고려할 필요가 있습니다. AI 감독의 일부 측면은 감사위원회의 업무와 더 부합하는 것으로 보입니다. 이러한 정합성을 고려하면, 감사위원회의 현재 기술 유창성 및 편의성 수준을 고려하는 것이 바람직합니다. 예를 들어, 감사위원회의 전통적인 거버넌스 영역을 고려할 때 재무보고에서 AI 사용을 감독하는 것이 현명할 수 있습니다.<sup>6</sup>

In other parts of AI oversight, it may be less clear whether the audit committee is a “good fit.” For example, the impact of generative or natural language AI on the workforce may be more aligned with the oversight of the compensation/talent committee or the full board.

The “temporary assignment” of AI to the audit committee may make sense for other reasons, as well. First, AI remains an emerging technology and is likely to continue to change rapidly. Second, there is extensive governmental interest in AI, which may result in legislation that will require adjustments in its oversight. Thus, determining now that AI, or aspects of AI, should be overseen by another committee or committees may turn out to be premature.

An audit committee might choose to assess its AI risk tolerance across oversight areas such as auditing, financial reporting, and internal control functions. It may be helpful to contextualize that analysis by comparing it to other areas of the company. For example, company divisions that routinely use technology enhancements in client-facing operations may have a higher appetite for risk. But a higher risk tolerance in operational settings does not necessarily correlate with how risks are viewed when it comes to financial reporting impacts.

An important part of the AI governance puzzle for the audit committee is assessing risk. But, at least for now, this task is currently made more difficult by a shifting regulatory landscape. Governments and regulators around the world are considering whether regulation and policy can address AI risks. Their progress toward developing and enacting policies and regulations over AI is uneven across the globe and in different stages of development and enactment. And to make things more complex, stakeholder groups—shareholders, customers/clients, employees, suppliers, and community—all have varying and sometimes conflicting expectations around use and governance of AI. For these reasons, there may be a benefit to continuously assessing AI risks and benefits over waiting for emerging and future legislative proposals or regulatory guidance. But to accurately make such continual assessments, it’s important that the audit committee and the board have sufficient knowledge to ask questions around the organization’s adoption and use of AI.

## QUESTION POTENTIAL AUDIT COMMITTEE OVERSIGHT QUESTIONS TO CONSIDER

- ▶ What are the company’s current and potential future use cases for AI, and do any of them have an impact on financial reporting or other audit committee oversight areas?
- ▶ Has management considered opportunities to use AI that may enhance or improve financial reporting processes?
- ▶ What processes are, or will be, used to evaluate dependencies that may arise in other areas where the audit committee may have primary oversight, like cybersecurity or data management?
- ▶ Are processes for use of AI congruent with the company’s risk appetite in terms of level of proactiveness and mitigation strategy?
- ▶ Given the speed of AI technology development, are existing processes being assessed and updated with appropriate frequency?

AI 감독의 다른 영역에서는 감사위원회가 “적합한” 조직인지 여부가 덜 명확할 수 있습니다. 예를 들어, 생성형 또는 자연어 AI가 인력에 미치는 영향은 보상/인재위원회 또는 이사회 감독과 더 적합할 수 있습니다.

감사위원회에 AI 감독 책임을 '임시로 부여하는 것'은 다른 이유에서도 타당할 수 있습니다. 첫째, AI는 여전히 새로운 기술이며 계속해서 빠르게 변화할 가능성이 높습니다. 둘째, AI에 대한 정부 차원의 관심이 높아지면서 AI 감독을 조정하는 법률이 제정될 수 있습니다. 따라서 지금 AI 또는 AI의 일부를 다른 위원회가 감독해야 한다고 결정하는 것은 시기상조일 수 있습니다.

감사위원회는 감사, 재무보고, 내부통제 기능과 같은 감독 영역 전반에서 AI 리스크 수용 범위를 평가할 수 있습니다. 이러한 분석을 회사의 다른 영역과 비교하여 맥락을 파악하는 것이 유용할 수 있습니다. 예를 들어, 고객 대면 업무에서 향상된 기술을 일상적으로 사용하는 부서는 리스크에 대한 수용 수준이 높을 수 있습니다. 그러나 운영 환경에서의 높은 리스크 수용도는 재무보고에 미치는 영향과 관련하여 리스크를 평가할 때 항상 상관관계가 있는 것은 아닙니다.

감사위원회를 위한 AI 거버넌스 퍼즐의 중요한 부분은 리스크를 평가하는 것입니다. 하지만 적어도 현재로서는 변화하는 규제 환경으로 인해 이 작업이 더욱 어려워지고 있습니다. 전 세계 정부와 규제 기관은 규제와 정책이 AI 리스크를 해결할 수 있는지 고민하고 있습니다.

AI에 대한 정책과 규정을 개발하고 제정하는 것은 전 세계적으로 개발 및 제정 단계도 다르며 불균형 하게 이루어지고 있습니다. 그리고 상황을 더 복잡하게 만드는 것은 이해관계자 그룹(주주, 고객/클라이언트, 직원, 공급업체, 커뮤니티) 모두 AI의 사용과 거버넌스에 대해 다양하고 때로는 상반된 기대치를 가지고 있다는 점입니다. 이러한 이유로 새로운 입법 제안이나 규제지침을 기다리는 것보다 AI 위험과 이점을 지속적으로 평가하는 것이 이점이 있을 수 있습니다. 그러나 이러한 지속적인 평가를 정확하게 수행하기 위해서는 감사위원회와 이사회가 조직의 AI 도입 및 사용에 관해 질문할 수 있는 충분한 지식을 갖추는 것이 중요합니다.

## QUESTION 잠재적 감사위원회 감독이 고려해야 할 질문

- ▶ 회사가 현재 및 잠재적인 미래에 활용할 수 있는 AI 사례는 무엇이며, 이 중 재무보고 또는 기타 감사위원회 감독 영역에 영향을 미치는 것이 있습니까?
- ▶ 경영진은 재무보고 프로세스를 강화하거나 개선할 수 있는 AI 활용 기회를 고려하였습니까?
- ▶ 감사위원회가 주요 감독을 담당하는 사이버보안 또는 데이터 관리와 같이 다른 영역에서 발생할 수 있는 의존성을 평가하기 위해 어떤 프로세스가 사용되거나 사용될 예정입니까?
- ▶ AI 사용 프로세스가 사전 대응 수준 및 완화 전략 측면에서 회사의 리스크 선호도와 일치합니까?
- ▶ AI 기술 개발 속도를 고려할 때, 기존 프로세스가 적절한 빈도로 평가되고 업데이트되고 있습니까?



Brian Cassidy



Ryan Hittner



Krista Parsons

**Brian Cassidy** is an Audit & Assurance partner with Deloitte & Touche LLP and the US Audit & Assurance Trustworthy AI leader.

**Ryan Hittner** is an Audit & Assurance principal with Deloitte & Touche LLP and the US Artificial Intelligence & Algorithmic Assurance coleader.

**Krista Parsons** is an Audit & Assurance managing director with Deloitte & Touche LLP. She is also the Governance Services coleader and the Audit Committee Program leader for Deloitte's Center for Board Effectiveness.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see <http://www.deloitte.com/about> to learn more.

# 기업지배기구발전센터 Contact



**김한석 파트너**

Partner / Audit & Assurance,  
Center for Corporate Governance Leader  
[hansukim@deloitte.com](mailto:hansukim@deloitte.com)



**박재환 교수**

기업지배기구발전센터 자문위원 /  
중앙대학교 경영학부 교수



**김학범 파트너**

Partner / Risk Advisory  
[hbkim@deloitte.com](mailto:hbkim@deloitte.com)



**유승원 교수**

기업지배기구발전센터 자문위원 /  
고려대학교 경영대학 교수



**정현 파트너**

Partner / Audit & Assurance  
[hyunjeong@deloitte.com](mailto:hyunjeong@deloitte.com)



**장정애 교수**

기업지배기구발전센터 자문위원 /  
아주대학교 법학전문대학원 교수



**오정훈 파트너**

Partner / Audit & Assurance  
[junoh@deloitte.com](mailto:junoh@deloitte.com)



**기업지배기구발전센터**

Center for Corporate Governance  
[krccg@deloitte.com](mailto:krccg@deloitte.com)