KPMG

Auditing artificial intelligence

kpmg.com

AI risks are affecting all organizations

Artificial intelligence (AI) is no longer a distant future—it's here, transforming industries at an unprecedented pace, bringing both game-changing opportunities and profound risks that no organization can afford to ignore. As AI continues to evolve, organizations must navigate a complex landscape of risks, that have the power to disrupt operations and erode trust, including:

Security and privacy: The use of generative AI poses security and privacy risks, which could result in data breaches, reputational damage, or privacy regulation violations. Growing threats lie from increasing sophistication and the speed of malware and cyberattacks.

Data management: Generative AI presents potential risks to data management, including quality, integrity, and bias. If not managed properly, it could result in inaccurate or biased outcomes, leading to legal liabilities, loss of client trust, and reputational damage.

Intellectual property: Lack of legislation defining ownership of AI-generated content may result in the inability to obtain copyright of content produced. Additionally, unclear terms of use may result in unintended violation of intellectual property rules.

Regulatory and professional standards: Regulators have not provided clear guidance on the use of generative AI. Navigating regulatory requirements and adhering to our professional standards may pose challenges due to unclear guidance.

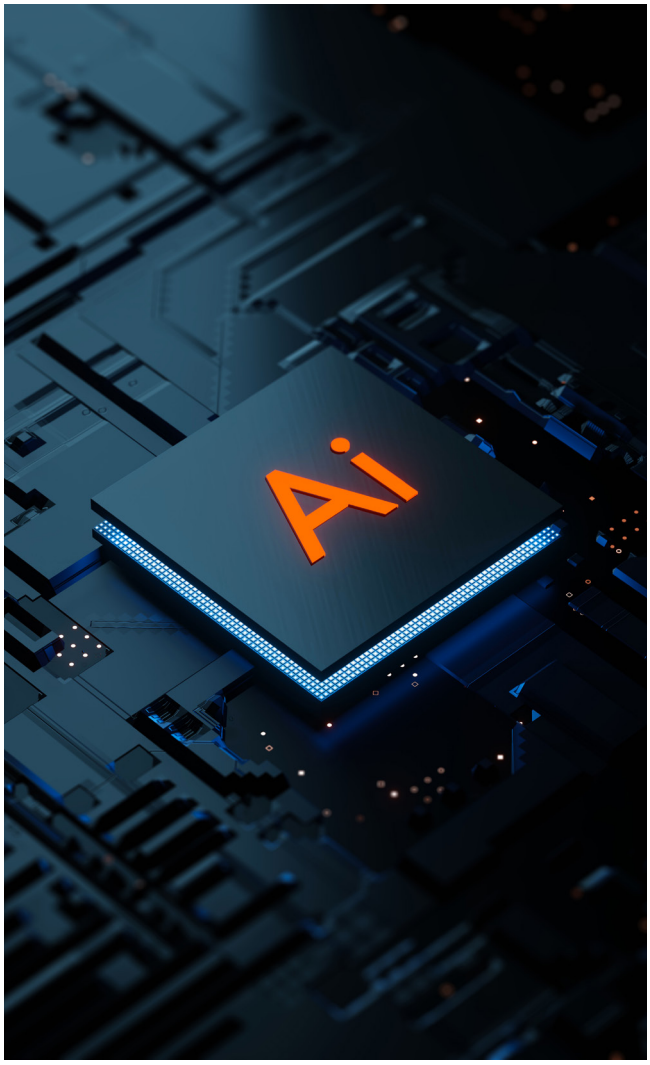
Policy: Organizations must amend existing IT policies by identifying scenarios for use and aligning with data governance and ethical standards, and provide adequate training to users. Failure to do so may result in policy violations, legal liabilities, and ethical concerns.

Brand and marketing: May perpetuate or amplify existing biases in the marketing and branding. Can result in negative impact on brand image and market share. An overreliance on AI-generated content may lead to a lack of creativity and originality in marketing campaigns.

How the internal audit function can add value

Internal audit can take a two-pronged approach to working with the organization by providing both consulting and assurance services, depending on the needs of the organization at the given time:

- For an organizations just beginning its AI program, internal audit may begin with an "in-flight" or "pre-assurance" assessment to provide valuable insights while the program, governance function, or a particular use case is still being established (i.e., consulting with the second line of defense as they set standards for the program).
- For an organizations further along in its AI journey, internal audit can perform audits to evaluate the effectiveness of the controls implemented as part of the AI program. These audits could include security and privacy reviews, AI governance model and framework, and postdeployment reviews.



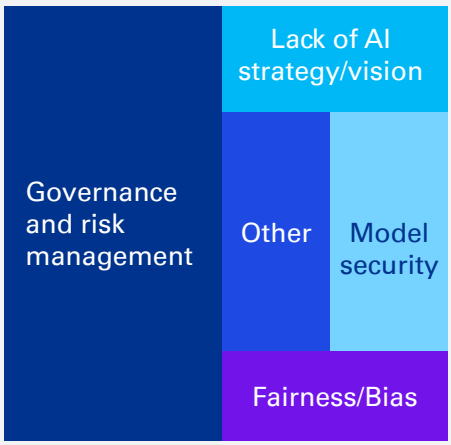
21%
of audits will focus on AI, the highest among all areas

What the market is telling us

- AI
- Regulatory compliance
- Application modernization
- Business modernization

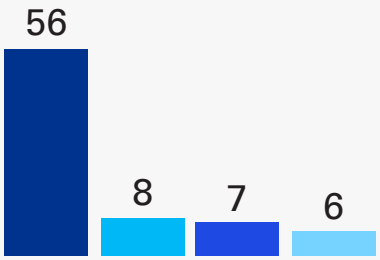
53%
of audits will focus on governance and risk management

Unique risk focus areas for 2025



56%
of teams do not feel prepared to audit AI

Areas where teams feel less prepared



- AI
- Cloud strategy
- Application modernization
- Data governance

38%
Believe external training will help the most with addressing internal audit's skill set gap

33%
Of internal audit teams lack technical knowledge of generative AI models and risks

21%
need AI skills for internal audit purposes

Source: KPMG hosted the Ask Experts Knowledge Cast series in January 2025. KPMG polled 1,500 professionals who hold various internal audit and risk positions at their respective companies.

Developing focus area for AI auditing

As AI becomes increasingly integrated into organizations, various types of AI audits and reviews have emerged to ensure transparency, fairness, security, and compliance—each serving a unique role in evaluating the effectiveness of AI programs. The following are examples of these audits and reviews.

AI use case intake process

Evaluates the processes for identifying, prioritizing, and approving AI use cases within the organization

AI governance model

Assesses the overall governance and risk management structure that oversees AI initiatives within an organization

AI framework and policy

Assesses the policies, procedures, and frameworks guiding AI development and deployment

AI governance workshops

Interactive sessions with key stakeholders to educate them on AI governance leading practices

AI security and privacy

Focuses on the security and privacy aspects of AI systems to ensure security risks are appropriatly considered and managed

Third-party/Vendor management reviews

Review the processes for selecting and managing AI vendors, as well as the processes for managing the introduction of AI within vendor provided products and services

AI solution pre/post-deployment assessments

Evaluate the readiness, performance, and impact of AI systems before and after deployment

Data governance reviews

Examine the data governance and management practices related to AI and assess compliance with relevant data protection regulations (e.g., General Data Protection Regulation, California Consumer Privacy Act) as well as data quality controls over data consumed by AI models

AI governance

Based on our experience, AI program reviews have been scoped in modules. This has allowed a focused approach on specific pain points or discovery requirements to provide stakeholders such as boards and audit committees with the right insight into an organization's AI program:

- **AI governance:** AI governance model: Assess the overall governance and risk management structure overseeing AI initiatives.
- **AI framework and policy:** Review the policies and frameworks guiding AI development and deployment.
- **AI governance workshops:** Facilitate interactive sessions on AI governance leading practices.
- **Vendor management:** Reviews the processes for selecting and managing AI vendors.

AI development and deployment

- **AI use case intake process:** Evaluates the process for identifying and prioritizing AI use cases.
- **AI solution pre/post-deployment assessments:** Assess the performance and impact of AI systems before and after deployment.

AI security and privacy

- **Data governance reviews:** Examine data management practices related to AI compliance with data protection regulations.
- **AI security and privacy:** Focuses on the security and privacy aspects of AI systems.

AI program

- **AI maturity assessment:** Evaluates the AI program using a Capability Maturity Model Integration from AI strategy to deployment and optimization of AI solutions against industry leading practices.

Auditing the AI governance model

The risk

- Unclear roles and responsibilities
- Outdated or inefficient policies
- Misaligned program roadmap
- Inadequate risk management

Our approach

- **Review governance model:** Assess roles, responsibilities, structure, and charters
- **Evaluate policies and protocols:** Assess against industry standards, evaluate implementation and communication
- **Compare program roadmap:** Review activities and timelines, assess strategic alignment
- **Assess AI framework:** Review principles, risks, controls, AI development lifecycle

The value

- **Clarity and accountability:** Establish clear roles and responsibilities
- **Efficiency and transparency:** Improved policy adherence and communication
- **Strategic alignment:** Ensur the roadmap aligns with business goals
- **Enhanced control:** Optimized AI development lifecycle and risk management

How KPMG can help

- **Experience in AI auditing:** Leverage our broad knowledge and experience
- **Tailored AI solutions:** Customized to fit your organization's needs
- **Strengthened AI governance:** Help ensure alignment and compliance
- **Enhanced cybersecurity:** Protect your AI systems
- **Skilled audit teams:** Bridge skills gaps with training

Contact us

Richard Knight
US IT Internal Audit Leader
KPMG LLP
E: raknight@kpmg.com

Diana Griffin
Trusted AI Director
KPMG LLP
E: dianagriffin@kpmg.com

Nana Amonoo-Neizer
Trusted AI Director
KPMG LLP
E: namonooneizer@kpmg.com

Kristy Hornland
Trusted AI Director
KPMG LLP
E: khornland@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**