AI in investigations – Navigating risks and unlocking new capabilities

With the rapid spread of AI, a new era for internal investigations has started.

Artificial intelligence (AI) is no longer a future-facing concept; it is a present-day reality with far-reaching implications across the business landscape. Changes are also very noticeable in the field of internal investigations. Traditionally rooted in manual reviews, interviews and process tracing, investigations are now being transformed by a new generation of technology-driven capabilities.

Since board members have fiduciary duties such as the duty of care, loyalty and oversight, it is increasingly important to understand and act on how AI is reshaping the nature of fraud risk and the strategies used to uncover it. AI is not only changing how investigations are conducted, but also why they are needed in the first place. It is enabling more sophisticated forms of misconduct while simultaneously offering powerful tools to detect, investigate and respond to such threats with unprecedented speed and precision.

Boards should consider that AI is raising the bar which has key implications on both fraud prevention and post-incident response. Oversight of this evolution must be proactive and strategic, not reactive.

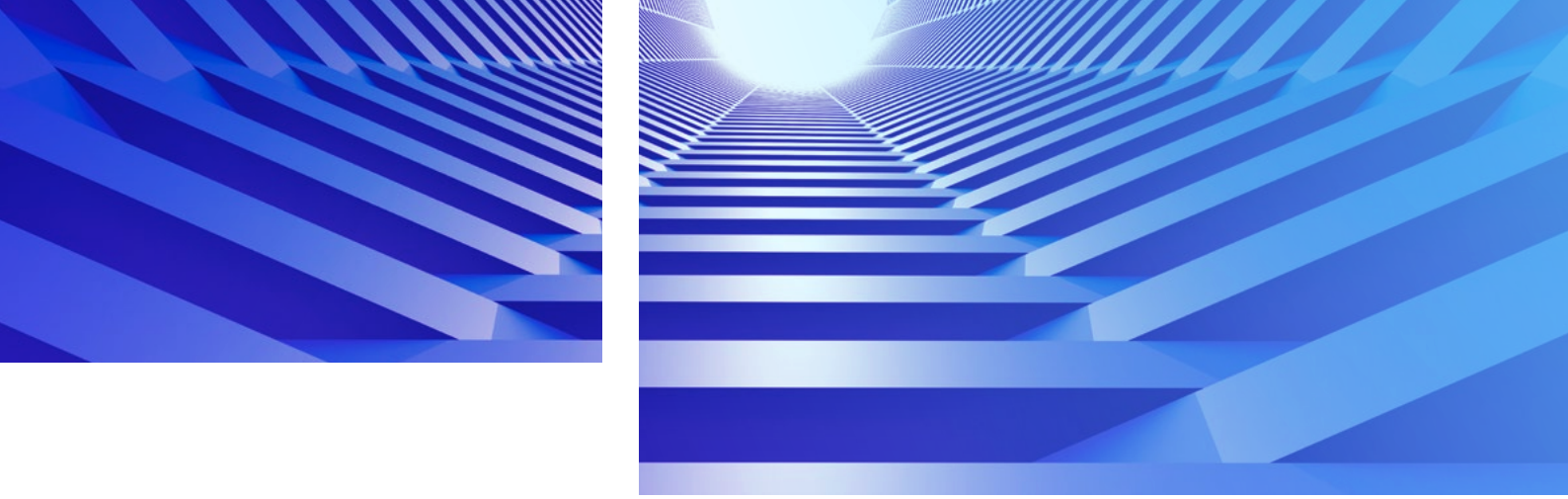
Double-edged sword: AI as both threat and tool

1. The threat landscape is evolving

As AI capabilities become more accessible, so too does their potential for misuse. Bad actors are leveraging AI to execute fraud schemes that are more convincing, easier to replicate and harder to detect than ever before.

Some examples include:

- **Deepfakes and synthetic media:** One of the most alarming developments is the use of AI-generated audio and video to impersonate real individuals. In early 2024, a finance professional at a multinational company was deceived into transferring USD 25 million after a video call with what appeared to be the company's CFO. However, it was a deepfake, skillfully created to mimic the CFO's appearance and voice. Attacks such as this exploit trust in visual and auditory cues, rendering traditional safeguards ineffective.



- **Voice cloning:** With just a few seconds of recorded speech, AI can replicate a person's voice with remarkable accuracy. Fraudsters are using this to impersonate senior executives and approve wire transfers or authorize sensitive actions. Voice cloning undermines verbal authentication processes and exposes a new layer of vulnerability in internal controls.
- **AI-assisted phishing and social engineering:** Generative AI tools are being used to draft highly convincing emails that mimic an individual's communication style. Unlike traditional phishing attempts, these messages are grammatically correct, context-aware and targeted. They can even include references to recent meetings or corporate initiatives, making them far more likely to succeed.

These developments increase exposure to financial loss, reputational damage and regulatory scrutiny. More importantly, they raise concerns about the effectiveness of current internal controls, employee training and incident response protocols. Boards must ensure that their organizations are adapting to this changing threat environment, not just with new technologies, but with updated governance and risk strategies.

2. AI as a force multiplier for investigations

Fortunately, AI is also enhancing the tools available to those tasked with uncovering and responding to fraud. When implemented responsibly, AI can enable investigations to move faster, dig deeper and draw conclusions with greater confidence. For example:

- **Anomaly detection:** Machine learning algorithms can analyze vast datasets to detect unusual transactions or behavioral patterns. These models are not restricted to predefined rules; they learn from past data to identify subtle signals that human reviewers might miss. For example, irregularities in vendor payments or overlapping travel expense claims can be flagged in real time for further investigation.
- **Behavioral analytics:** AI can build profiles of typical employee behavior based on factors such as system access patterns, transaction history or email activity. When a user deviates significantly from this baseline, the system can raise an alert. These insights surpass traditional threshold models, allowing for real-time detection of insider threats or breaches.
- **Natural language processing (NLP):** Investigative teams often face the daunting task of reviewing thousands of communications across multiple platforms. NLP technologies can sift through emails, chat logs and meeting transcripts to extract relevant topics, identify emotional tone and detect sentiment shifts over time. This allows investigators to pinpoint key individuals, events and timelines quickly, without relying solely on keyword searches.
- **Generative AI:** These tools, when applied with caution and effective prompting, can support case summarization, document organization and cross-referencing of findings. Investigators can use AI to connect seemingly unrelated data points and uncover hidden relationships, helping to build a coherent narrative more efficiently.

By leveraging these technologies, investigative teams can improve the quality and speed of their work while reducing the burden on overstretched compliance functions. However, this also requires investment in training, infrastructure, and ethical oversight to ensure tools are used effectively and responsibly.

Implications for boards

Boards should not treat AI as a purely technical or operational issue. The integration of AI into investigations and compliance functions brings fundamental governance questions to the surface. These include ethical considerations, data security risks and the broader accountability framework surrounding automated decision-making.

Three key areas warrant board-level attention:

1. Preparedness and prevention

Boards should ensure that management has conducted a thorough risk assessment of how AI could be used maliciously within the organization, including the exploitation of publicly available data and weaknesses in internal processes. It is equally important to ensure that appropriate safeguards are in place to regulate the organization's own use of AI tools. This includes guidance on acceptable use, data privacy and responsible experimentation with generative models.

2. Detection and response capability

Internal investigation functions must be equipped with the right tools and skills to detect fraud early and respond effectively. This may involve investing in forensic analytics platforms, upskilling teams in data science or developing partnerships with third-party technology providers. Boards should inquire whether the organization has a clear escalation process for AI-detected anomalies and whether it can act quickly when digital evidence surfaces.

3. Governance and trust

Transparency and fairness are essential when using AI in investigations. Automated outputs must be auditable and explainable. Boards must verify that ethical standards, control systems, and oversight processes are ready to support responsible AI implementation in this context. Regular reporting on AI use in risk management, compliance monitoring, and investigations should become part of the board's agenda.

Regulatory context

Regulators are taking note of the growing influence of AI on fraud prevention and compliance. Organizations that fail to integrate AI responsibly may soon find themselves falling short of legal and regulatory expectations.

Two concrete examples where this is happening are:

- In September 2024, the U.S. Department of Justice (DoJ) updated its Evaluation of Corporate Compliance Programs to reflect emerging technologies. The revised guidance encourages companies to leverage AI and data analytics in their compliance and fraud detection activities, while also stressing the importance of monitoring, training and ethical deployment of such tools.
- The Economic Crime and Corporate Transparency Act of 2023 (ECCTA) introduced, under Section 199, a new corporate offence of "failure to prevent fraud" under UK law. A company may now be held criminally liable where an economic crime is committed for its benefit and it did not have adequate anti-fraud procedures in place. The UK Home Office published guidance on 6 November 2024 offering directions on how to comply. This sets a clear expectation for companies to implement "reasonable procedures" to prevent fraud committed by associated persons. While the guidance does not explicitly reference AI, the scope and scale of required risk management make it evident that advanced technologies such as AI and machine learning are increasingly necessary to meet the bar for compliance. It should be noted that starting on 1 September 2025, even Swiss companies may face criminal liability under this UK law if they fail to implement adequate anti-fraud procedures.

Boards must therefore consider whether their organizations are meeting not only the letter of regulatory expectations, but also the spirit, by demonstrating a proactive, risk-based approach to emerging threats and capabilities.

A strategic imperative for boards

AI is not just a technical innovation; it represents a strategic turning point. Companies that view AI purely as a compliance obligation risk falling behind. Those that approach it as a driver of competitive advantage – through better risk detection, more efficient investigations and stronger controls – stand to benefit.

For boards, this means asking deeper questions about readiness, investing in investigative capacity and fostering a culture of ethical innovation. AI is already changing how internal investigations are conducted. The question is no longer if it will impact your organization, but how prepared you are to respond.

This is the time to lead, not follow.

Authors

Bob Dillen
Partner, Head of Forensic
KPMG Switzerland

+41 58 249 31 11
bdillen@kpmg.com

Cindy Hofmann
Director, Forensic
KPMG Switzerland

+41 58 249 56 25
cindyhofmann@kpmg.com

This article is part of KPMG's Board Leadership News.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center offers support and guidance to board members. We equip you with the tools and insights you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business. In addition, we help you to connect with peers and exchange experiences.

Learn more at **kpmg.ch/blc**