SHADOW AI

THE FRAUD RISK NO ONE APPROVED

By Alia Noor, FCMA, CGMA, MBA

Associate Partner, Taxation & Compliance Advisory

Alia Noor is a Forbes Finance Council member and international speaker with 18+ years across audit, risk, governance, taxation, and compliance.

Alia says that employees trust that AI-generated summaries are accurate, that reports reflect the underlying data, and that analytical outputs are complete and verifiable. But what happens when the technology shaping those decisions operates outside the governance, outside any oversight, and outside visibility itself?

That is the challenge of **Shadow AI.** Organizations can govern only what they can see. For decades, governance frameworks have rested on that principle — management monitors systems it approves, auditors evaluate controls they can access, and fraud examiners investigate what leaves evidence behind. Artificial Intelligence is beginning to challenge that assumption.

Employees increasingly use AI tools to work faster, often without formal approval, risk assessment, or oversight. This is Shadow AI: the use of AI outside established controls. The greatest AI risk is not the model an organization approved; it may be the one it never knew existed.

When Visibility Disappears:

Traditional technology implementations follow a predictable path. Systems are evaluated, approved, tested, monitored, and governed. Risks are assessed before deployment and access is controlled. Shadow AI bypasses that process. Employees may use AI tools to analyze data, draft communications, summarize contracts, review reports, or support decisions without involving IT, Compliance, Risk Management, or Internal Audit.

PROFESSIONAL INSIGHT:
SHADOW AI
THE FRAUD RISK NO ONE APPROVED

While each activity may appear harmless, management often has little visibility over what information is being processed or how AI-generated outputs are influencing decisions.

Unlike approved enterprise systems, many AI tools operate outside established control environments. Employees can access them through personal devices, web browsers, or free subscriptions within minutes.

As a result, organizations often struggle to answer simple but important questions:

- Which AI tools are being used?
- Who is using them?
- What information is being uploaded?
- How are outputs being validated?
- What controls exist to prevent misuse?

For fraud examiners and auditors, this lack of visibility creates a significant blind spot.

And fraud risks thrive in blind spots.

A Governance Breach Before a Fraud Occurs: One of the most dangerous misconceptions surrounding Shadow AI is the belief that no harm has occurred unless a fraud has taken place.

Consider a simple example: A finance manager uploads a vendor master file into a publicly available AI platform to identify duplicate suppliers and unusual payment trends. The objective is legitimate. The analysis may even produce useful insights.

However, within minutes, supplier records, bank account details, payment histories, tax registration numbers, and commercially sensitive information have left the organization's controlled environment.

No fraud has occurred.

No money has been stolen.

No control failure has been identified.

Yet a significant governance breach has already taken place.

The risk lies not only in what AI can do, but also in what organizations may unknowingly expose when using it.

The reality is that many organizations will discover their AI governance weaknesses only after a regulatory inquiry, data breach, fraud investigation, or reputational incident.

A New Category of Fraud Risk

Fraud risks evolve whenever technology changes.

PROFESSIONAL INSIGHT:
SHADOW AI
THE FRAUD RISK NO ONE APPROVED

Artificial Intelligence is creating new opportunities for both efficiency and abuse.
Sensitive information that was once protected within organizational systems may suddenly exist outside them. More concerning is the ability of AI to generate highly convincing content. Fraud has always relied on creating believable stories. Artificial Intelligence can now generate those stories faster, more convincingly, and at a scale never previously possible. Professional-looking reports, supplier correspondence, supporting documentation, business justifications, and persuasive narratives can all be produced within seconds.

For fraud examiners, the challenge is no longer simply determining whether documentation exists. The challenge is determining whether it can be trusted.

The Rise of Synthetic Reality

Historically, organizations operated on a simple assumption: seeing was believing. Artificial Intelligence is weakening that assumption. Deepfake technologies can replicate voices, images, videos, and communications with remarkable accuracy.

Criminals have already used AI-generated voices to impersonate executives and request urgent fund transfers.
Imagine receiving a call from a senior executive requesting an immediate payment. The voice sounds familiar. The language feels authentic. The request appears legitimate. Yet the individual speaking may not exist at all.
As synthetic content becomes more sophisticated, organizations will need to reconsider controls that rely solely on familiarity, verbal confirmation, or visual evidence.
In the past, fraudsters needed stolen credentials. Tomorrow, they may need only a convincing synthetic identity.

Why Governance Matters

The response to Shadow AI should not be fear.
Artificial Intelligence has enormous potential to strengthen organizations. Internal auditors can analyze entire populations of transactions. Compliance teams can identify emerging risk indicators. Fraud examiners can detect patterns that traditional reviews might overlook.

PROFESSIONAL INSIGHT:
SHADOW AI
THE FRAUD RISK NO ONE APPROVED

Used responsibly, AI can significantly enhance fraud detection capabilities.
However, powerful tools require effective governance. Effective AI governance requires clear policies, protection of sensitive data, independent review of AI-generated outputs, visibility over adoption across the organization, and clear accountability for decisions supported by AI.
Without these foundations, organizations may find themselves using powerful technology without fully understanding the risks it introduces.

The Role of Internal Audit

Internal Audit has a critical role in helping organizations navigate this emerging risk landscape. Its role is not to own AI governance. Responsibility remains with management. Instead, Internal Audit should provide independent assurance regarding whether appropriate governance structures exist and whether they are operating effectively.
Key questions include:

- Does the organization have a formal AI governance framework?
- Are employees aware of approved and prohibited uses?
- Is sensitive information being shared with external platforms?
- Are AI-generated outputs independently validated?
- Have AI-related risks been incorporated into enterprise risk assessments?

These questions are not about restricting innovation. They are about ensuring innovation occurs within an environment of accountability and control.

Looking Ahead

Shadow AI represents a unique challenge because it combines powerful capabilities with limited visibility and rapidly evolving risks. It exists at the intersection of technology, governance, compliance, and fraud risk.
The future of AI governance may ultimately depend on a simple principle:
Organizations can govern only what they can see. Fraud risks thrive where visibility is limited. Controls operate where transparency exists. Shadow AI sits somewhere in between. The question is not whether Artificial Intelligence is already being used within your organization. The question is whether your governance framework arrived before it did.

STUDENT ARTICLE

STANDING AT THE THRESHOLD

By Aiham Talal Al Nairi · Assurance Officer (Internal Audit), OQ SAOC · SQU Graduate 2025

I belong to a generation that never knew a purely analogue investigation, so data analytics and digital forensics are not a transformation to us; they are simply the starting line. Yet the more I learn, the more I understand how much I am inheriting from the fraud fighters who came before — people who built the standards, the ethics, and the community I am now joining.

That is the odd privilege of arriving now. I stand between two worlds: the hard-won wisdom of a generation that defined what integrity looks like, and a frontier of AI-generated documents, synthetic voices, and risks no one has fully mapped yet. What reassures me is that the core has not changed — the tools evolve, but the mission of protecting honest people from those who would deceive them is exactly the one my mentors describe.

Technology may decide how we fight fraud. It will never decide why. I do not yet have decades of cases behind me. What I have is a commitment to carry the legacy forward, and the curiosity to meet the frontier head-on.

When I tell people I studied accounting and am now stepping into a role fighting fraud, they often picture ledgers and paper trails. I have come to realise I am entering the profession at a stranger moment than that — one where the trail itself may be fabricated by a machine.

My degree was not a fraud programme as such; it was a BSc in Accounting and Finance. But looking back, fraud was never absent from it. Almost every course carried its own thread of ethics, fraud awareness, and risk — a case study here, a red flag there — until the mindset became second nature.

THE FRAUD SENTINEL

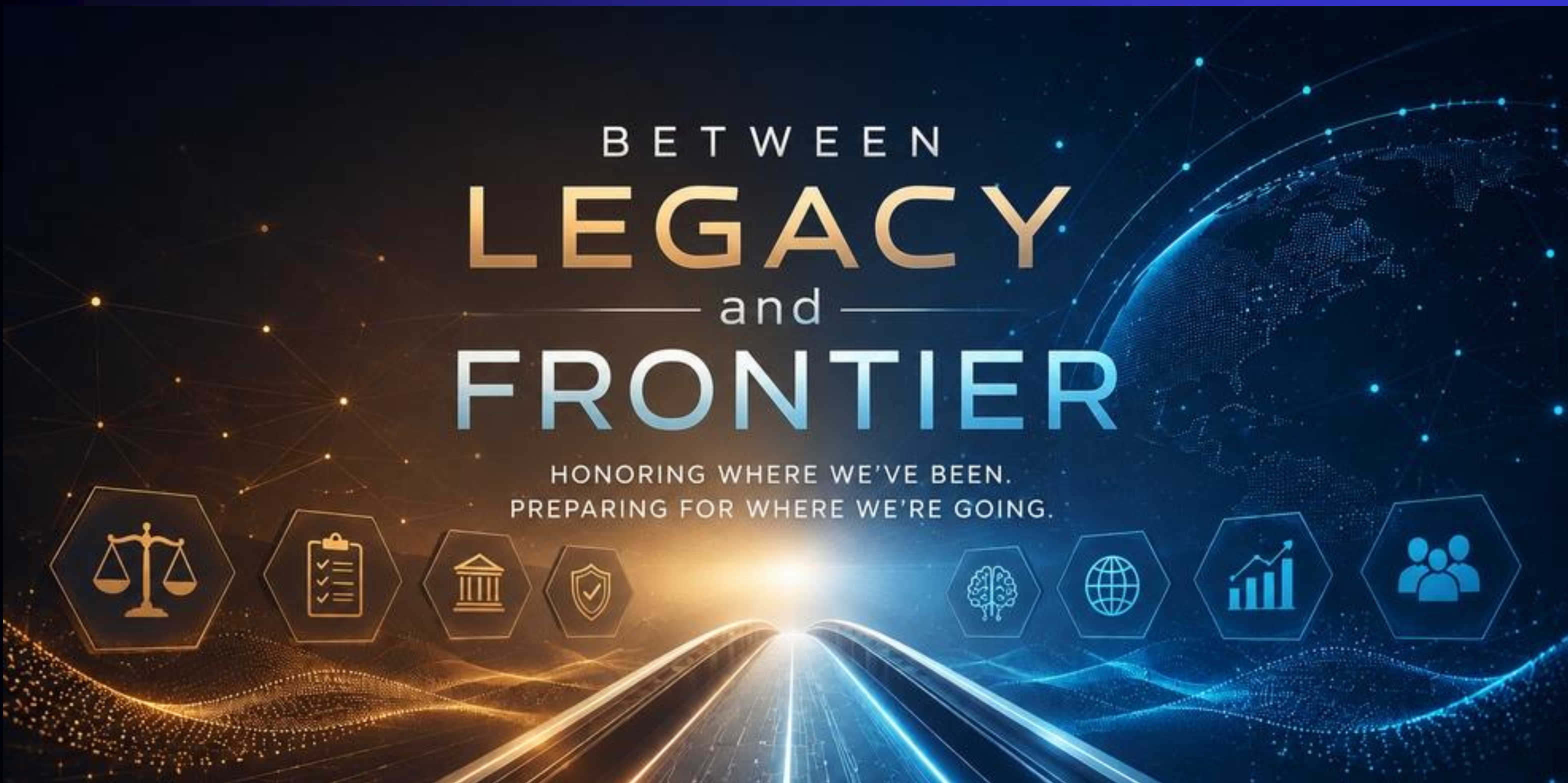
10 YEARS ACFE™
Association of Certified Fraud Examiners
جمعية محققي الاحتيال المعتمدين – فرع سلطنة عُمان
تحت مظلة كلية الدراسات المصرفية والمالية

MONTHLY NEWSLETTER

June 2026 | Issue #6

Cover Feature:

In Conversation with John Gill — the Retiring ACFE Global President



Inside this issue

SHADOW AI: THE FRAUD RISK NO ONE APPROVED – BY ALIA NOOR, FCMA, CGMA, MBA

STUDENT ARTICLE — STANDING AT THE THRESHOLD, BETWEEN LEGACY AND FRONTIER