Deloitte.

Together makes progress



From leads to action:
A faster way to run corporate investigations

FRAUD INVESTIGATION & INCIDENT RESPONSE

The challenge

Legal and compliance teams face an overwhelming volume of signals. Whistleblower tips, transaction monitoring alerts, expense anomalies, and third-party risk flags arrive faster than any team can effectively triage by hand. Every credible lead must still be investigated: evidence must be gathered, policy citations located, and a defensible recommendation written before any action can be taken. This manual process is slow, often inconsistent across investigators, and difficult to scale when caseloads spike.



Our point of view

Deloitte has developed a reusable framework—not a single-purpose tool—that is designed to transform how investigations move from a potential lead to a defensible action. It combines network analysis, machine learning, and agentic AI to compress weeks of manual review into minutes, while keeping a human investigator firmly in control of every decision. This approach was originally tested on massive-scale federal health care fraud data and has a direct architectural application for corporate investigations including employee conduct, anti-bribery and corruption, trade compliance, procurement fraud, and insider risk.



How it works: A three-phase approach

1. Connect the dots

Most organizations already collect the signals that matter—they often just exist in different systems, are owned by different teams, and are rarely analyzed together. The framework links records across the business into a single, unified picture. For example:

- **HR**: Disciplinary history, performance reviews, organizational changes, and offboarding timing.
- **Finance**: Expense reimbursements, vendor payments and credits, and approval overrides.
- **Procurement / TPRM**: Vendor onboarding data, ownership records, and third-party risk assessments.
- **Cyber/IT**: Device activity, access logs, and communication metadata.
- **Legal**: Prior investigations, litigation holds, and whistleblower reports.
- **Compliance**: Policy attestations, training completions, and audit findings.

Connecting signals that are normally reviewed in isolation is what surfaces hidden relationships—such as shared bank accounts, addresses, or approval chains—before an investigator even opens a file.

2. Prioritize and recommend

A machine learning model scores and groups similar cases, so one confirmed pattern can automatically surface every other instance. Each group comes with a recommended action based on how similar cases were historically resolved and what your policies require. Every recommendation is fully explainable, not a "black box," providing transparency into the factors behind each decision.

3. Build the evidence package

For any case an investigator chooses to pursue, AI agents assemble a complete evidence package. This includes the facts uncovered, mapped line-by-line to the specific policy each fact supports, along with a draft recommendation. This automates what used to be days of manual record-pulling and memo-writing, completing it in minutes. The investigator's role then shifts to validating and contextualizing every package before any action is finalized.

Built for how compliance teams actually work

Catch problems while you write the policy, not after it's exploited:

Beyond detecting misconduct, the same AI can stress-test a proposed policy or control before it's finalized. It can simulate how an individual might exploit ambiguous language and flag loopholes or other unintended consequences upfront. This shifts compliance work from reacting to violations to designing more durable rules from the start.

Monitor risk continuously, not just at your next audit cycle:

Most compliance monitoring is periodic—annual attestations, quarterly reviews, scheduled recertifications. But business doesn't stand still. Vendor ownership can change, employee conflicts may emerge, and new relationships form between review cycles. Continuous monitoring flags these changes as they happen, instead of waiting for the next scheduled review.

Ask questions in plain English, not just accept pre-scored leads:

Investigators can query the data directly—for instance, "show me every vendor terminated for cause who re-registered under a new name"—without needing a data analyst or predefined search terms. This supports testing new hypotheses and surfacing schemes for which no rule has been written.

Build institutional memory across cases and business units:

A pattern learned in one investigation, region, or business unit can inform every future case, preventing each investigator from having to start from scratch. Over time, the system—and your organization—gets smarter about how misconduct actually appears in your business.

Why this matters for legal and compliance

- **Speed to Insight**: Cases that once took weeks to substantiate can now be scoped in hours.
- **Consistency and Defensibility**: Every recommendation is tied to specific, citable policy language and explainable factors, building organizational trust and a strong position if a decision is challenged.
- **Scalability**: One validated pattern can surface dozens of related cases with the effort it used to take to close a single one.
- **Sharper Policy Signal**: Recurring fact patterns often indicate a policy is hard to enforce, giving compliance leadership a data-backed case for updating it.
- **Better Metrics for Leadership**: Track more than just financial recoveries. Measure time-to-detection, investigative capacity freed up, and the value of potential losses mitigated, not just harm caught after the fact.



Responsible by design

This is not a black box making decisions on your behalf. The framework is built around core governance principles: it is secure, privacy-preserving, transparent, explainable, fair, accountable, and reliable. Every evidence package is human-reviewed before action, and the framework is designed to sit alongside your existing case management and data systems rather than replace them.



Getting started

Our approach begins with a focused pilot. We help you catalog the data, policies, procedures, and adjudicated decisions that can be used to train the models and agents. We then apply the framework to a defined slice of your case backlog, validate the outputs against outcomes your team already trusts, and expand from there. The architecture plugs into the systems you already run—case management, HRIS, financial systems—so scaling beyond the pilot doesn't require rebuilding your investigations stack.

The underlying capability has already demonstrated its ability to detect coordinated, multi-actor schemes and compress evidence-gathering timelines in a large-scale federal fraud environment. Applied to corporate investigations, it gives legal and compliance teams a way to do more with their current resources—with a level of reliability and audit trail that every stakeholder can trust.

Who to contact



Jen Larson
Partner
Deloitte Financial Advisory Services LLP
jenlarson@deloitte.com



Rob Biskup
Managing Director
Deloitte Financial Advisory Services LLP
rbiskup@deloitte.com



Ryan Colabello
Senior Manager
Deloitte Financial Advisory Services LLP
rcolabello@deloitte.com

Deloitte.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document 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 advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte Financial Advisory Services LLP, which provides forensic, anti-fraud, litigation, dispute, and computer forensic advisory services; and Deloitte Transactions and Business Analytics LLP, which provides eDiscovery, analytics, and a wide range of advisory and analytic services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting. Deloitte does not provide legal services and will not provide any legal advice or address any questions of law.

Copyright © 2026 Deloitte Development LLC. All rights reserved.

MAKING AN IMPACT THAT MATTERS since 1845