Deloitte.

Together makes progress



From fragmented defenses to an adaptive fraud operating model

FRAUD OPERATING MODEL

The challenge

Fraud is no longer contained within a single process, control, channel, or team. It can span external threat actors, employees, customers, vendors, third parties, external threat actors, cyber-enabled activity, financial reporting, procurement, payments, and digital channels. Accountability for identifying and responding to fraud is often distributed across functions. Further, Generative and agentic artificial intelligence (AI) is increasing the speed, scale, and sophistication of some fraud schemes, raising the importance of timely detection and coordinated response to mitigate.

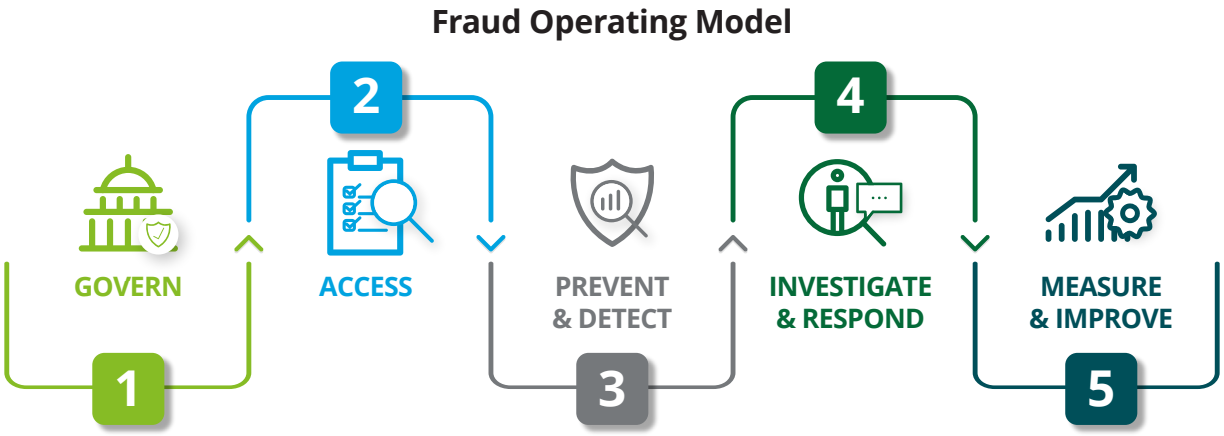
The scale, persistence, and evolving nature of fraud reinforce the need for an enterprise-wide programmatic response. Organizations need more than individual fraud capabilities. They need an integrated fraud operating model that establishes clear accountability, connects disparate signals, embeds prevention and detection into business processes, enables coordinated investigations and response, and continuously learns from fraud events.



Our point of view

An effective fraud program is a cohesive operating model, not a collection of controls.

We view an effective fraud operating model having five mutually reinforcing principle components:



The model is informed by the leading principles while extending them with the operating-model mechanisms (e.g., decision rights, cross-functional ownership, data flows, and feedback loops) needed to make those principles work in practice.

Fraud risk extends across the enterprise, including financial and non-financial activities. Therefore, fraud risk management should be integrated with governance, enterprise risk management and internal control across the enterprise, too.

The result is a closed-loop fraud defense: risk intelligence informs controls; controls generate signals; signals drive investigations; investigation outcomes inform remediation; and lessons learned continuously reshape the organization's risk assessment and controls. When these capabilities are connected, an organization operates through shared data, coordinated governance, common processes and cross-functional decision-making. Models become increasingly predictive, dynamic and adaptive, using real-time intelligence, AI-enabled analytics, enterprise learning and performance insights to anticipate emerging risks from data signals and proactively adjust controls.

The objective is not simply to identify more fraud. It is to reduce the opportunity for fraud, identify emerging schemes earlier, respond consistently, recover losses where appropriate, and make the organization harder to exploit over time.



How it works: The five components

1. GOVERN
Establish accountability and decision rights

The foundation of a fraud operating model is clear accountability. The board and senior management establish expectations for integrity, ethical behavior and fraud risk management, while management translates those expectations into policies, roles, decision rights and operating procedures. Components of governance include:HR: Disciplinary history, performance reviews, organizational changes, and offboarding timing.

- Board and Audit Committee oversight;
- Executive accountability;
- Fraud risk owner(s);
- Roles and accountability across Finance, Internal Audit, Legal, Compliance, Risk, HR, Procurement, Cyber, and Security;
- Investigation ownership and escalation paths;
- Decision rights for case disposition;
- Third-party and ecosystem responsibilities;
- Data ownership and access;
- Technology and AI model governance; and
- Reporting and management information.

As the fraud operating model matures, fraud risk management becomes embedded in the broader strategic planning and decision-making rather than operating solely as a standalone control function. Fraud intelligence can inform decisions around new markets, products, customers, third parties, business transformation and technology investment, while risk-based metrics and incident learning inform leadership priorities.

The fraud function should not operate as an isolated center of expertise. Instead, organizations should establish a model in which central fraud leadership communicates standards, methodology, and oversight while business functions retain accountability for risks within their operations and processes.

2. ASSESS
Build a dynamic view of fraud risk

Fraud risk assessments should serve as a dynamic and iterative process for identifying and assessing fraud risks relevant to the organization, including fraudulent financial and non-financial reporting, asset misappropriation and corruption. Such assessments should consider the following:

- Internal incidents and control failures;
- External threat intelligence and typologies;
- Business, product, and process changes;
- Third-party and ecosystem relationships;
- Transaction, identity, cyber, and behavioral signals; and
- Regulatory and technology developments.

As the fraud operating model matures, risk assessment evolves from a periodic exercise into a continuously refreshed and increasingly predictive view of fraud exposure. Technology, including as assisted by AI and agentic AI, should be selected based on the risk, decision, data, and workflow it is intended to support.

3. PREVENT & DETECT
Design controls around how fraud actually occurs

Fraud-control activities should be selected, implemented, and monitored based on identified risks. As the model matures, detection can progress from known-rule monitoring toward analytics that identify emerging behaviors and relationships, correlating signals across the enterprise and continuously improving as new fraud patterns are identified. Organizations should consider ingestion of data from trusted sources (e.g., public-private data sharing consortiums, regulators, law enforcement) to inform risk signals.

Preventive controls include segregation of duties, approval and controls, access controls, vendor/customer onboarding requirements, identity verification, and payment controls.

Detective controls include ongoing transaction monitoring, behavioral analytics, anomaly detection, data matching, and pattern recognition.

Emerging technologies provide organizations with AI-, machine-l earning- and advanced-analytics-enabled services and accelerators designed for ongoing fraud risk assessment, monitoring and training.

4. INVESTIGATE & RESPOND
Turn signals into action

This component establishes a consistent and confidential process to intake, triage, investigate, and resolve potential fraud—and to turn findings into prevention and control improvements. Fraud events require prompt, competent and confidential review, investigation and resolution. Investigation outcomes can become a source of enterprise learning rather than remaining isolated within individual cases. Root-cause analysis, recurring patterns and lessons learned can inform fraud risk assessments, control design, detection logic, training and business-process improvements across functions.

Intake mechanisms include hotlines, employee reports, monitoring alerts, customer complaints, and regulatory inquiries.

Triage process analyzes areas such as potential financial impact, regulatory and legal exposure, customer harm, and evidence availability.

Investigations utilize case management, forensic analyses, interviews, transaction review data analytics, corporate intelligence, and eDiscovery.

Response, as appropriate, may involve containment, corrective or disciplinary action, recovery, control remediation, policy or process changes, third-party action, and escalation to regulators or law enforcement.

AI opportunity: Agentic AI may help investigators gather and organize evidence, surface relationships and linked patterns, compare facts with policies, summarize findings, and recommend next steps. Human investigators remain accountable for judgments and decisions.

5. MEASURE & IMPROVE
Make the fraud program self-correcting

Regular monitoring and periodic independent reviews assess whether the fraud operating model is working as intended, whether risks are changing, and where intervention is needed. This differentiates a fraud operating model from a collection of fraud capabilities. Metrics should be interpreted in context: an increase in detected fraud may indicate stronger detection, while lower reported fraud may reflect under-detection rather than improvement. As maturity increases, reporting can progress from static reporting toward interactive, real-time and exception-driven views of fraud risk and performance. Organizations can combine internal performance data with external benchmarks and predictive indicators to identify emerging issues, communicate proactively with stakeholders and inform strategic fraud-management decisions. Below are select considerations.

- Risk exposure: high-risk schemes identified; residual risk; emerging typologies
- Detection: time to detection; alert-to-case conversion; detection source; false-positive rate
- Response: time to triage; investigation cycle time; case backlog; escalation timeliness
- Impact: estimated loss prevented; loss recovered; control improvements; repeat incidents
- Program health: training completion; control effectiveness; analytics coverage; open remediation items



The enabling layer: People + process + data + technology

An effective fraud operating model depends on the integration of people, processes, data and technology across every stage of the fraud lifecycle.

People provide the judgment, subject-matter expertise and accountability required to identify risk, investigate allegations and make defensible decisions, while clearly defined processes establish consistent approaches for risk assessment, control design, monitoring, intake, triage, investigation, remediation, recovery and lessons learned.	**Technology**, including analytics, network analysis, text analytics, digital forensics, automation and AI (generative, predictive and agentic), can then help organizations analyze those signals at scale, prioritize activity and augment human decision-making.	**Processes** operate cross-functionally through shared data and coordinated governance. Further, they can become increasingly predictive, automated and adaptive, enabling enterprise-wide learning and proactive changes to controls and business operations.	**Data** connects signals that may otherwise remain fragmented across financial, HR, procurement, customer, cyber, communications, case-management and external intelligence sources, creating a more complete view of relationships, behaviors, and emerging risks.

The opportunity is not to optimize one component in isolation, but to connect them so that intelligence generated in one part of the organization informs decisions elsewhere.



Built for how organizations actually work

Connect what already exists: Most organizations already have relevant fraud capabilities distributed across multiple functions. The challenge is connecting them.

Move from periodic to connected: Link risk assessment, control performance, investigations, and external intelligence so that important signals inform action more quickly.

Turn every investigation into institutional knowledge: Every investigation should strengthen risk assessment, controls, detection logic, training, or monitoring.

Use AI to augment, not replace, fraud professionals: The operating model should define ownership, validation, monitoring, access controls, and prioritization for AI-enabled activities.

Responsible by design

Technology and AI can improve the speed and scale of fraud prevention and investigation, but it also introduces risks related to accuracy, explainability, bias, privacy, security, and data access. A responsible model therefore combines human accountability with appropriate validation, monitoring, access controls, and data minimization.

A modern fraud operating model should therefore incorporate AI governance, privacy and data minimization, cybersecurity, model validation, explainability, human oversight, and appropriate access controls. This is particularly important in fraud investigations, where AI-enabled tools may process sensitive employee, customer, financial, communications, or investigative information.

These safeguards become especially important where AI-generated output could influence an investigation, employee action, customer decision, or regulatory response. Human oversight and explainability can help ensure that AI outputs are treated as decision-support rather than unquestioned conclusions, while controls over data access, use, and monitoring can help reduce privacy and confidentiality risks.

Getting started

Organizations should not view a mature fraud operating model as a single technology implementation or fixed end state. The maturity journey should build progressively from defined governance and processes to measurable cross-functional capabilities and, ultimately, to predictive and continuously improving fraud management. The appropriate target state will depend on the organization's risk profile, operating environment, regulatory obligations, data availability, and strategic priorities.

- **Establish the baseline**: Map existing governance, risk assessments, controls, monitoring, reporting channels, investigations, data, analytics, metrics, and gaps across the five components.
- **Identify the highest-value use case**: Select one fraud risk where improved prevention, detection or investigation could demonstrate measurable value. Potential examples include procurement and payment fraud, and customer or claims/charge back fraud. Short, targeted pilots can help organizations test value in an existing risk area before scaling.



- **Connect the data**: Determine which existing sources can provide useful fraud signals. For example: Finance, procurement, HR, cyber, case management, and external data from trusted sources. The objective is not necessarily to create a new data platform. It is to determine how existing information can be connected and analyzed to identify relationships, anomalies and emerging patterns.
- **Introduce AI where it solves a defined problem**: Introduce AI only where it solves a defined problem, improves a specific decision or workflow, and can be governed appropriately. Start with targeted use cases rather than 'AI transformation.'
- **Establish success measures before scaling**: A pilot should not simply demonstrate that the technology works. Organizations can consider:
  - **Speed**: time to identify, triage, and investigate;
  - **Quality**: actionable leads, false positives, output accuracy, user adoption; and
  - **Outcomes**: losses identified or recovered, control gaps, repeat incidents, and capacity released.
- **Scale through the operating model, not just the technology**: Once a use case is validated, expand through governance, risk assessment, controls, investigation, measurement, and continuous learning—enabled by people, process, data, and technology

Fraud operating model resilience is built by connecting capabilities, not simply by adding another tool. Organizations can begin by mapping what exists, selecting a priority use case, connecting relevant signals, measuring outcomes, and scaling what works. The operating model should be reviewed and enhanced routinely as new fraud risks emerge.

Who to contact



Sam Parish
Principal
Deloitte Financial Advisory LLP
saparish@deloitte.com



Rory Heenan
Senior Manager
Deloitte Financial Advisory Services LLP
rheenan@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, a subsidiary 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.

Copyright © 2026 Deloitte Development LLC. All rights reserved.

MAKING AN IMPACT THAT MATTERS since 1845