Transforming fraud risk assessment through data and economic crime integration

Deloitte | A Middle East Point of View - Spring 2026 | Transforming fraud risk assessment

The traditional approach to fraud risk assessment, characterized by process walkthroughs, organizational data analysis, and stakeholder perspectives, is fundamentally inadequate for today's complex and rapidly evolving fraud landscape. Many organizations continue to rely on methodologies designed for an era in which fraud was less sophisticated, predominantly internal in nature, slower-moving, and more predictable. However, in today's environment, these approaches have become increasingly unsustainable.

Modern fraud has transformed dramatically. Criminals now operate with unprecedented sophistication, leveraging advanced technology, Artificial Intelligence, and coordinated networks to execute attacks at scale and velocity that traditional controls cannot detect or prevent. Rather than isolated incidents of individual fraud, organizations now face organized fraud networks operating across multiple jurisdictions and business units. According to the Association of Certified Fraud Examiners' (ACFE's) 2026 Report to the Nations, frauds carried out by three or more perpetrators caused median losses almost 6 times greater than those carried out by a single perpetrator.[1]

Simultaneously, fraud has become inseparably linked with broader financial crimes: money laundering, sanctions evasion, terrorist financing, corruption, and embezzlement. Fraud is no longer an isolated risk; it is often the entry point or enabling mechanism for larger financial crime schemes.

The imperative for transformation
The imperative is clear: organizations must transition from traditional, process-focused internal fraud identification to data-driven, proactive fraud risk assessment integrated with comprehensive financial crime monitoring. This transformation requires a multi-faceted approach, which includes:

- **Holistic data integration:** Combining internal transaction, customer, and employee data with external intelligence sources to create a comprehensive risk picture.
- **Organizational alignment:** Breaking down silos between fraud, compliance, and financial crime teams to enable coordinated detection and response.
- **External fraud typology assessment:** Identifying and evaluating potential threats from external actors exploiting organizational vulnerabilities through cyber intrusion, social engineering, payment fraud, and other sophisticated tactics.
- **Stakeholder ecosystem perspective:** Extending risk assessment beyond internal sources to encompass customers, suppliers, third-party partners, and other external stakeholders, thereby identifying risks that traditional internal-focused approaches overlook.

Criminals now operate with unprecedented sophistication, leveraging advanced technology, Artificial Intelligence, and coordinated networks to execute attacks at a scale and velocity that traditional controls cannot detect or prevent

Deloitte | A Middle East Point of View - Spring 2026 | Transforming fraud risk assessment

- **Financial crime integration:** Recognizing fraud as part of the broader financial crime ecosystem and detecting cross-crime patterns that indicate sophisticated, multi-layered schemes.
- **Continuous monitoring capability:** Transitioning from periodic assessments and trigger-based updates to real-time data analytics and continuous risk monitoring.
- **Predictive analytics adoption:** Leveraging machine learning and Artificial Intelligence to identify emerging fraud patterns before they materialize into significant losses.

Modern fraud risk assessment approach

A modern fraud risk assessment approach begins by redefining fraud across two critical dimensions: internal versus external fraud, and fraud as part of the broader financial crime environment.

External fraud

External fraud risk assessment must be evaluated across multiple organizational dimensions:

- Product portfolio and service offerings exposed to external fraud vectors
- Customer segments and their associated fraud vulnerabilities
- Delivery channels (digital, physical, hybrid) and their inherent risks
- Geographic markets and regional fraud typologies
- Third-party relationships and partner ecosystem risks

Organizations should employ comprehensive data analytics to identify patterns across complete datasets, revealing anomalies and suspicious behaviors that traditional sampling methods inevitably miss

External fraud typologies should be identified through various industry publications, intelligence monitoring, regulatory guidance, and peer benchmarking. Once identified, these typologies must be assessed against the organization's specific dimensions to identify, assess, and document external fraud risks.

Internal fraud

Internal fraud assessment requires a fundamental shift from stakeholder-dependent approaches to data-driven, analytics-based methodologies:

Risk-based data analytics: Rather than relying on subjective stakeholder perspectives and sample-based data validation, organizations should employ comprehensive data analytics to identify patterns across complete datasets. This approach reveals anomalies and suspicious behaviors that traditional sampling methods inevitably miss.

Domain-specific risk identification: Fraud risks should be systematically identified across defined operational and technological domains, including software and system access controls, mobile application usage and authentication, Environmental, Social, and Governance (ESG) initiatives and greenwashing risks, cybersecurity vulnerabilities and digital asset protection, as well as financial transaction processing and reconciliation.

Cross-crime pattern detection: By recognizing fraud as part of the broader financial crime ecosystem, organizations can identify sophisticated schemes that would remain invisible to siloed, fraud-only systems. Cross-crime pattern detection reveals how fraud often serves as an enabler for money laundering, sanctions evasion, or corruption schemes.

The internal and external fraud risk assessments should be synthesized to represent a holistic picture of the fraud risk landscape facing the organization, enabling prioritized resource allocation and targeted control implementation.

Data-driven control assessment requires greater reliance on automated, system-enforced controls rather than manual, discretionary controls that are inherently inconsistent and subject to human error

Control assessment and effectiveness evaluation
An often overlooked aspect of traditional fraud risk assessment is the rigorous evaluation of control effectiveness. Conventionally, significant time and effort are devoted to identifying fraud risks, while assessing control effectiveness is delegated to control testing or assurance teams relying on sample-based testing methodologies. This fragmented approach identifies risks but often fails to determine whether existing controls can effectively mitigate them, leaving organizations vulnerable to the impact of already-recognized risks.

Data-driven control evaluation:
Control assessment must transition to comprehensive data analytics approaches. Machine learning models should be trained on control breakdowns, historical incident data, and operational patterns to evaluate control effectiveness on a real-time basis. This methodology enables:

- Continuous effectiveness monitoring rather than periodic testing cycles
- Automated control validation reducing reliance on manual, sample-based testing
- Predictive control failure identification before incidents occur
- Adaptive control recommendations based on emerging threat patterns

This data-driven assessment necessarily requires greater reliance on automated, system-enforced controls rather than manual, discretionary controls, which are inherently inconsistent and subject to human error.

Control behavior analysis

Beyond merely verifying the existence of controls, modern fraud risk assessment must evaluate how controls function in practice under real-world conditions. Control behavior analysis encompasses:

Consistency assessment: Evaluating whether controls operate uniformly across all transactions, users, and scenarios, or whether exceptions and workarounds undermine their effectiveness.

Adaptability evaluation: Assessing the control framework's capacity to respond to emerging fraud threats and evolving attack methodologies without requiring extensive manual reconfiguration.

Responsiveness measurement: Determining whether controls detect and respond to suspicious activities with sufficient speed to prevent or minimize losses.

Integration analysis: Evaluating how controls function within the organization's broader risk management framework and whether they operate in isolation or as part of a coordinated defense system.

By focusing on control behavior, organizations can identify weaknesses not apparent through traditional sample-based testing, enabling a more dynamic and proactive approach to fraud prevention and detection. This shift ensures that controls are not only present but are genuinely effective in mitigating identified risks, thereby reducing the organization's exposure to fraud.

Data-driven fraud risk dashboards and monitoring

Archaic fraud risk registers should be replaced with data-driven fraud risk dashboards allowing for fraud risks to be monitored on a real-time basis. Data-driven fraud risk assessment represents a fundamental shift from traditional, reactive approaches to proactive, analytics-based detection and prevention. Rather than relying on static rules and periodic audits, data-driven approaches leverage advanced analytics, machine learning, and continuous monitoring to identify fraud patterns in real-time.

This transition from traditional to data-driven fraud risk assessment is no longer optional; it is essential for effective fraud prevention in the modern financial landscape. The traditional fraud risk assessment model needs a complete overhaul from defining fraud to risk identification, control measures, and monitoring. Organizations that embrace integrated, data-driven practices will be better positioned to detect emerging threats, strengthen control effectiveness, and build more resilient fraud risk management capabilities.

Organizations that embrace integrated, data-driven practices will be better positioned to detect emerging threats, strengthen control effectiveness, and build more resilient fraud risk management capabilities

Endnote
1. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2026/2026-report-to-the-nations.pdf.

By **Karthik Prabhakar**, Partner, Deloitte Middle East, and **Faiza Qureshi**, Assistant Director, Forensic & Financial Crime, Deloitte Middle East