Deloitte.

Emerging fraud risks and preventive checklist

For Risk, Control, and Compliance leaders

As frauds evolve rapidly, staying ahead requires sharper vigilance and smarter frameworks. Leadership is often the first line of defence against these emerging frauds. Here are some of the key trends and regulatory developments that you could prioritise to strengthen your organisation's resilience to frauds.

AI-driven and deepfake fraud

Fraudsters use GenAI and deepfake technologies for impersonation and identity theft. Despite awareness efforts, incidents such as fabricated arrests and digital impersonations persist. Furthermore, there have been incidents where technology was used to create fake supporting documents for expenses or to falsely demonstrate the existence of ethics and compliance policies and frameworks to stakeholders. Organisations could:

- Enforce Multi-Factor Authentication (MFA) on critical systems and strengthen with biometrics to prevent spoofing and deepfakes
- Use AI models to identify anomalies in voice and video communications
- Use digital watermarking to verify authenticity
- Conduct regular proactive compliance risk assessments

Cybersecurity vulnerabilities

Phishing and social engineering attacks are leveraging GenAI to bypass traditional defences. Combined with weaknesses in critical infrastructure, cybersecurity has become a core compliance issue. Organisations could:

- Integrate real-time threat intelligence to counter phishing and social engineering attacks
- Update threat models to include AI-driven attack vectors
- Adopt a zero-trust architecture across all infrastructure and applications

Data privacy and protection

Data privacy has become central to an organisation's risk management strategy, especially with evolving global regulations. Leaders must revisit data governance frameworks, particularly for non-digital sources that may contain Personally Identifiable Information (PII). They could:

- Encrypt sensitive data end-to-end, both in transit and at rest
- Deploy Data Loss Prevention (DLP) tools across digital and physical environments
- Conduct periodic privacy impact assessments, review access controls, and compliance audits

Regulatory complexity and uncertainty

Rapid regulatory developments, coupled with delays in finalising guidelines, may create operational ambiguity - especially for global organisations managing cross-border compliance. Leaders need agile compliance programmes that adapt quickly without compromising governance standards. They could:

- Establish a centralised compliance dashboard to provide real-time visibility into regulatory adherence, audit trails, and risk indicators across all business units
- Automate compliance monitoring and reporting through tech-enabled platforms
- Implement cross-border compliance protocols to minimise risk and ambiguity

Conflict of interest (COI)

Even mature compliance cultures face lapses due to unclear interpretations of conflict of interest. Unmanaged conflicts can cause legal, financial and reputational damage. Organisations could:

- Enforce annual COI disclosures from employees and leadership
- Implement a comprehensive third-party risk management framework (Including end-to-end vendor lifecycle review i.e. from identification to processing of payments)
- Implement secure, anonymous, and independent whistleblower channels and policies that support reporting without fear of retaliation
- Deliver ethics training based on real-world scenarios to reinforce integrity

Proactive vigilance and adaptive controls are key to staying ahead of emerging fraud risks. Make fraud prevention a priority. Let's keep fraud out of the workplace.

International Fraud Awareness Week
16-22 November 2025

Connect with us

Nikhil Bedi
Leader – Risk, Regulatory & Forensic
Strategy, Risk & Transactions
Deloitte India
nikhilbedi@deloitte.com

K.V. Karthik
Leader – Forensic & Financial Crime
Strategy, Risk & Transactions
Deloitte India
kvkarthik@deloitte.com