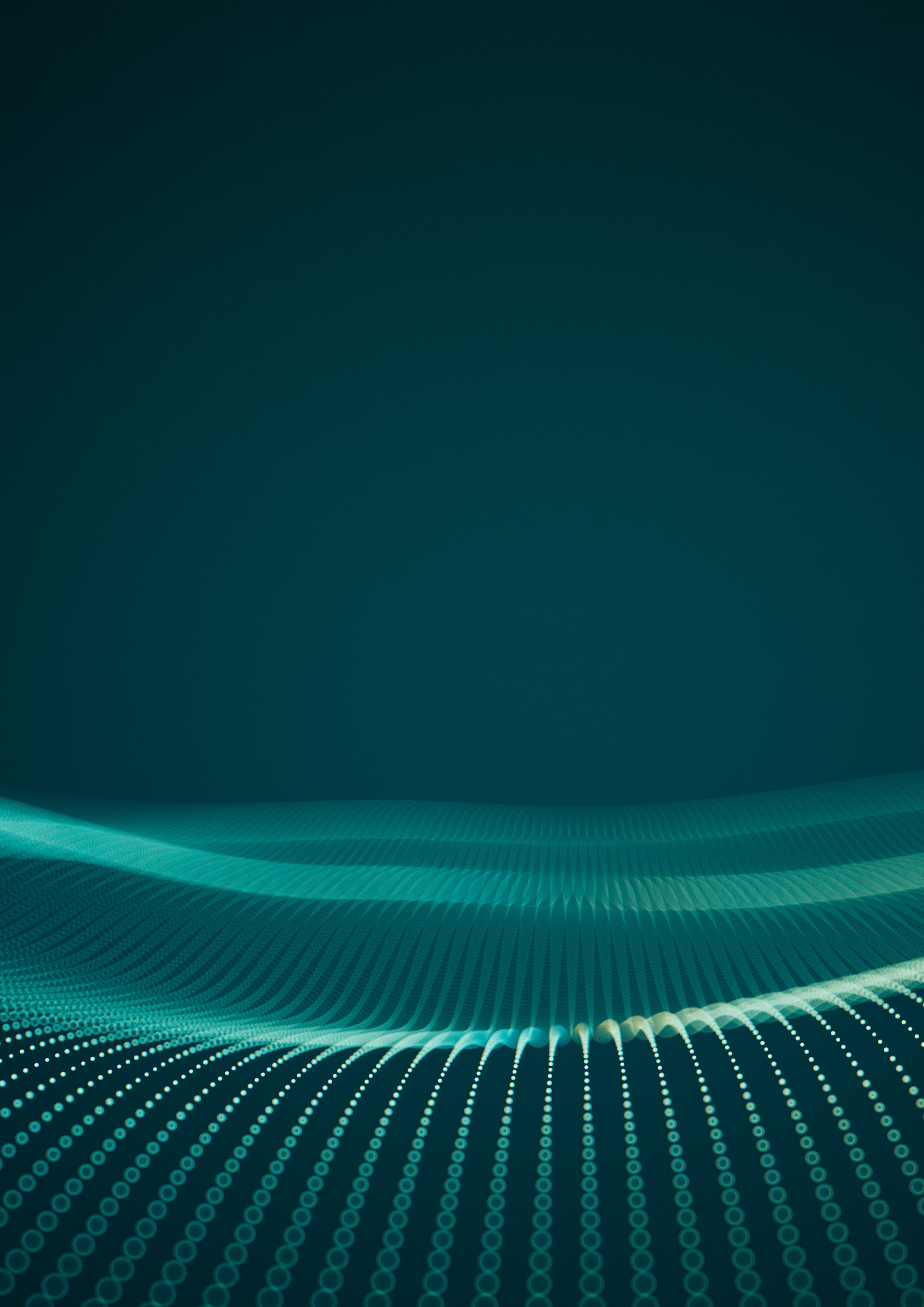
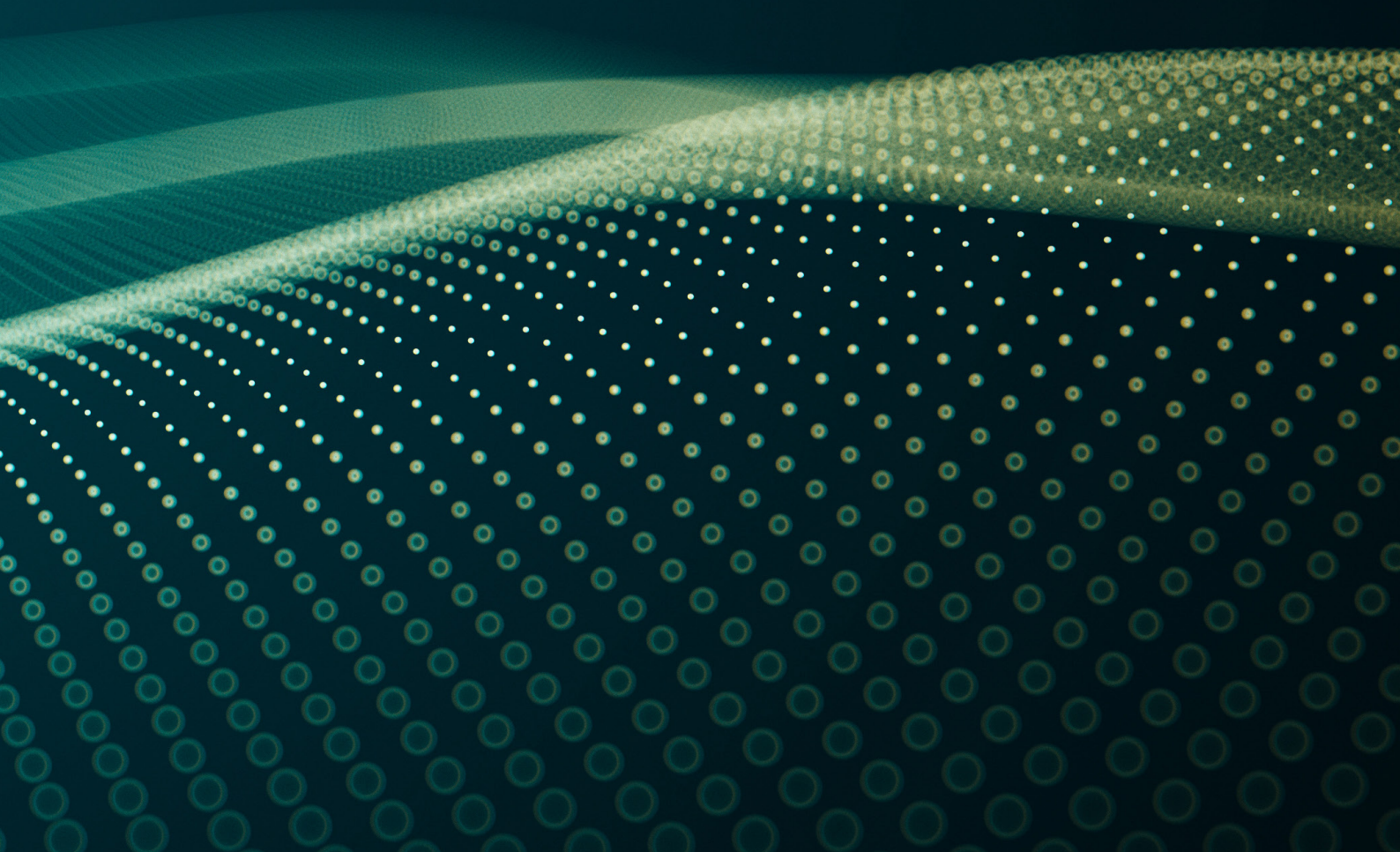
The fraud factor

The better the question.
The better the answer.
The better the world works.

Shape the future with confidence



Contents



Foreword - EY

Establishing fraud-resilient organizations through strategic integration of advanced technology

The business landscape is undergoing a dynamic transformation, driven by rapid adoption and global interconnectivity. Building a truly resilient organization now requires not only embracing innovation but using it to strengthen trust and integrity. At the same time, fraud risks are also evolving. Fraud has evolved from isolated incidents to systemic threats embedded in complex digital infrastructures. Sophisticated fraud schemes now pose significant financial, legal, and reputational risks to organizations.

EY and FICCI have developed this knowledge paper exploring how organizations can build robust fraud management frameworks by using multi-level compliance checks and strategic technology integration. It aims to outline key considerations for enhancing resilience through improved compliance and the thoughtful use of technology.

A reactive approach will never be enough to build a fraud-resilient organization. It often leads to crisis situations. By anticipating vulnerabilities and embedding integrity into every level of operations, organizations can proactively prevent fraud through regular checks. Implementing sector-specific fraud control mechanisms further enhances the approach by addressing industry-specific risks.

By developing systems that detect and deter wrongdoing while fostering trust among stakeholders, organizations can secure sustainable growth.

Arpinder Singh

India & Emerging Markets Leader,
EY Forensic & Integrity Services

Foreword - FICCI

As India navigates a rapidly evolving economic and regulatory landscape, the importance of organizational integrity has never been more pronounced. With rising instances of complex fraud, driven by digital transformation and global interconnectivity, building resilient institutions demands more than conventional compliance—it calls for strategic foresight, robust governance, and a culture of accountability. FICCI has consistently championed initiatives that strengthen trust and transparency in business, and this joint knowledge paper with EY is a timely reflection of our shared commitment to enabling ethical growth and sustainable development.

FICCI believes that capacity building and knowledge sharing are essential pillars in the fight against financial crime. As businesses scale, the risks they face grow more sophisticated, and therefore, our collective response must be equally agile and intelligent.

This report offers valuable insights into the anatomy of modern fraud, the vulnerabilities across sectors, and the imperative to integrate technology with risk management frameworks. It also highlights the need for proactive leadership, responsible corporate behaviour, and global-local harmonization in fraud prevention. I am confident this paper will serve as a guiding resource for industry leaders, compliance professionals, and policymakers alike in building future-ready, fraud-resilient enterprises.

Rajeev Sharma

Chair
FICCI Committee on Private Security Industry

The evolving fraud landscape

A comprehensive overview of current fraud trends and emerging threats

The global business environment is facing heightened integrity-related risks driven by the growing influence of AI, digital transformation, complex supply chains, and continuously evolving regulatory expectations. According to our Global Integrity Report 2024, 45% of organizations experienced significant integrity incidents in the past two years, including fraud, data breaches, or compliance violations. A whopping 93% of these incidents involved third parties, which underscores highlighting rising vulnerabilities in third-party vendor relationships and outsourced functions.

The ACFE Report to the Nations 2024, which surveyed 1921 real cases across 138 countries, confirmed that occupational fraud remains widespread. Common schemes include asset misappropriation, corruption and billing fraud, with a median loss of US$145,000 per case. Procurement fraud leads the charge, closely followed by deceptive practices in sales, distribution, e-commerce, inventory management, workforce operations and ethical breaches.

Digital transformation, without corresponding internal controls, has created exploitable gaps. Malicious actors exploit these vulnerabilities by manipulating systems, forging documents, and operating across departments with little oversight. When it came to factors that pose the greatest integrity risks for organizations over the next two years, conflicts of interest ranked as first most important factor. When it came to investing increased resources and budget to mitigate integrity risks, including compliance and fraud risks, Indian employees ranked financial crimes and money laundering as priorities.

Modern fraud schemes are devised to blend seamlessly into existing control environments, remaining undetected long enough to cause damage. Collusion among multiple actors

ensures that fraudulent activities are masked effectively, making detection increasingly difficult. The challenge is not merely to identify isolated incidents but to dismantle coordinated, strategic fraud networks. The tech-forward fraud landscape demands a proactive and intelligent approach to fraud prevention.

Examination of organizational fraud dynamics and vulnerabilities

Organizational fraud is becoming increasingly pervasive, complex and costly. Companies lose around 5% of their revenue to fraud annually, amounting to over US$5 trillion globally. Lack of internal controls or the override of existing controls contributes to over 50% of fraud cases. As per the Global Integrity Report 2024 – India edition, 92% of respondents agreed that the general public in India has higher expectations regarding workplace behavior, as compared to two years ago, and 83% respondents agreed that employee expectations of management conduct has risen significantly.

The willingness to compromise ethical standards for personal advancement is alarmingly prevalent across hierarchies. The EY report findings show that 38% of global respondents comprising board members, senior managers, managers and employees in large organizations and public bodies, are likely to engage in unethical behavior to further their careers. More concerning is that 67% of board members and 51% of senior management expressed the same readiness. As many as 62% of Indian respondents strongly agreed that unethical behavior is often tolerated when the people involved are senior or high performers. These findings highlight that ethical lapses are deeply embedded across the workforce. When personal gains are prioritized over integrity or misconduct is neglected, it erodes trust and blurs the boundaries, making it challenging for the organization to prevent unethical behavior. Organizations must reinforce ethical conduct at every level, close the say-do gap, and integrate integrity into the core of operations.

Analysis of recent regulatory updates and evolving compliance requirements

The regulatory landscape is evolving rapidly, shaped by domestic demands, global geopolitical shifts, and alignment with international laws and reforms. Governments are racing to regulate emerging technologies while balancing innovation and ethical safeguards. As many as 69% of Indian respondents strongly agreed that adapting to the speed and volume of regulatory changes can be challenging. Factors such as inflation, unemployment, exchange rates, global conflicts and trade tensions also make it difficult to conduct business with integrity.

The Digital Personal Data Protection Act marked a pivotal moment in India's privacy framework, mirroring the EU's GDPR and the US's sectoral data laws. Simultaneously, the surge in Artificial Intelligence adoption has prompted India to propose a National AI Safety Institute and regulatory frameworks. This move echoes the EU's AI Act and China's expanding AI governance. Amid geopolitical tensions and economic uncertainties, regulatory agility and ethical resilience will be key to navigating the next phase of corporate governance.

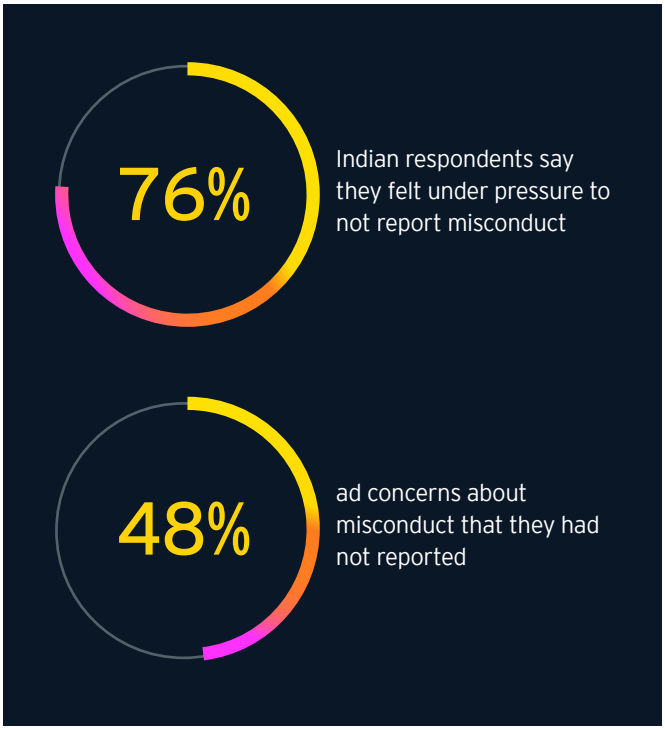
However, the Economic Survey 2024-25 emphasizes the critical role of deregulation in accelerating economic growth and employment. It advocates simplifying regulations and reducing compliance burdens to lower the cost of doing business. Environmental, Social, and Governance (ESG) compliance has gained strategic importance over the years and will continue to play a key role in shaping corporate strategies despite the ongoing debate. In India, SEBI's Business Responsibility and Sustainability Reporting (BRSR) framework continues to push companies to disclose sustainability metrics, in line with global efforts like the EU's Corporate Sustainability Reporting Directive (CSRD) and the US SEC's proposed climate disclosure rules. Meanwhile, Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations have tightened under RBI and ED oversight, in response to FATF's evolving guidelines. These shifts form part of a global crackdown on financial crimes, with increased emphasis on transparency, due diligence and real-time monitoring.

Anatomy of an investigation

Upholding rigorous reporting standards to ensure transparency and accountability

Upholding rigorous reporting standards is essential to cultivating a culture of transparency, accountability, and integrity within an organization. These standards are the backbone of effective governance, enabling stakeholders to access accurate, consistent and timely information that supports informed decision making. Leadership plays a vital role in setting and maintaining these standards. When leadership behavior does not align with its messaging, trust in internal reporting mechanisms erodes. 76% of Indian respondents reported feeling pressure against reporting misconduct, with 46% harboring unreported concerns.

Structured reporting frameworks—such as standardized templates, clear data validation protocols, and regular audit mechanisms— help ensure reports are factually sound and aligned with strategic goals. 54% of respondents cited a lack of training, awareness, and resources as key enablers of misconduct. This points to a need for continuous education, clear policies, and accessible reporting tools. Rigorous reporting is not just about operational efficiency, it is a strategic imperative that reinforces ethical standards, supports long-term sustainability, and builds a resilient, high-performing organization.

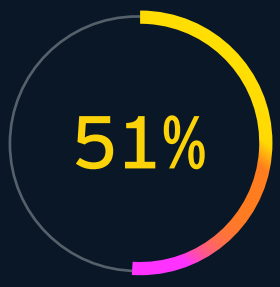


The critical role of robust governance frameworks in fraud prevention and detection

62% of survey takers from India—the highest across countries—admitted regulators had acted against their organization for breaching integrity standards or regulations in the last two years. Yet almost half of the respondents said they had witnessed behavior by other employees that would damage the organization's reputation if it were known externally, but still no action was taken against them. There is no denying that a robust governance framework plays a pivotal role in both the prevention and detection of fraud, and serves as the foundation for ethical conduct, risk management and organizational integrity. This framework helps guide employee behavior and decision-making across all levels of an organization. When these frameworks are well-designed and consistently enforced, they help create a culture of transparency and responsibility in the long run, inadvertently making it difficult for fraudulent activities to go unchecked.

Understanding the fraud triangle—pressure, opportunity and rationalization—is key to designing resilient governance frameworks. Effective governance frameworks are built on multiple levels of oversight—internal audits, risk assessments, whistleblower mechanisms and compliance monitoring—which work in tandem to identify vulnerabilities, flag anomalies, and ensure that corrective actions are taken promptly. This proactive approach to fraud risk management, with controls embedded into every function, instead of a reactive one, makes the organization resilient and enables it to act quickly towards resolution. Technology also plays a critical role in facilitating real-time data analysis and automated alerts that enhance the speed and accuracy of fraud detection.

When senior management supports ethical practices and reinforces the importance of integrity, it makes a powerful statement. This alignment between values and actions builds stakeholder trust and protects reputation.



Indian respondents revealed facing or witnessing some form of retaliation or adverse consequences towards someone who reported misconduct through their organization's whistleblowing mechanism

Maximizing the effectiveness of whistleblowing mechanisms to uncover fraudulent activities

The whistleblowing mechanism is one of the most crucial tools for uncovering fraudulent activities and fostering a culture of transparency and accountability. ACFE's report found that 43% of fraud cases were uncovered through tips, making it the leading detection method—three times more effective than internal audits or management reviews. At the core of a robust whistleblowing framework are clear policies that categorize what qualifies as fraud, misconduct or unethical behavior. When communicated effectively across all levels of the organization, these policies ensure that employees understand their rights and responsibilities. Many organizations are already adopting whistleblowing to further their compliance efforts, which is reflected in the way 32% respondents concur that people are now more concerned about reporting misconduct than they were two years ago. By setting up multiple, accessible channels for reporting concerns, organizations can encourage participation in the fight against misconduct.

Trust is the cornerstone of every organization and to build trust in their whistleblowing program, companies must guarantee confidentiality by implementing strict protocols to safeguard the identity of whistleblowers and ensure they are protected against retaliation. 76% of Indian respondents of the GIR survey admitted that they felt under pressure to not report misconduct, which does not come as a surprise because 51% respondents revealed facing or witnessing some form of retaliation or adverse consequences towards someone who reported misconduct through their organization's whistleblowing mechanism. Other reasons for not reporting instances of misconduct include a lack of confidence that the issue will be addressed, loyalty to the organization, pressure from the management to not report, loyalty to colleagues, and a lack of responsibility to address the issue.

35% of respondents shared that they felt people were afraid to use the whistleblower hotline, leading to the conclusion that the success of a whistleblowing program lies in adequate training. The message from the top should also reinforce the organization's commitment to ethical conduct and support for whistleblowers. When employees believe their concerns will be taken seriously and that they will be protected, they are more likely to come forward with valuable information.

To conclude, whistleblowing mechanisms must be integrated into a broader fraud risk management strategy. This involves regularly reviewing and improving reporting systems, analyzing whistleblower data for patterns, and using insights to strengthen internal controls. Being vigilant also means ensuring that investigations are led by qualified experts who can assess claims impartially and thoroughly. . By treating whistleblowing as a proactive tool rather than a reactive measure, companies can detect fraud early, minimize financial and reputational damage, and reinforce a culture of integrity.

Tech and innovation

As technology continues to permeate every aspect of our lives, the associated risks are evolving just as rapidly. CHROs and HR professionals now face an emerging risk landscape that includes challenges such as fraudulent employment records, moonlighting, falsified credentials, the use of deepfakes in online interviews and dual employment. In this dynamic environment, adopting a strategic, technology-driven approach to risk management is crucial. This approach prioritizes thorough employment background checks and the development of comprehensive policies to detect and address emerging risks effectively.

Managing today's HR and compliance risks requires more than traditional approaches. Technology now plays a critical role in detecting anomalies, investigating complex issues, and responding swiftly to potential threats. Along with deep domain knowledge, organizations need to employ advanced analytics to conduct effective background checks, identify red flags, and monitor emerging risks. From e-discovery and cyber investigations to continuous monitoring, technology-driven solutions are helping build stronger compliance, resilience, and integrity into everyday operations.

Let us take the risk of moonlighting, for example. In India, the legal position on moonlighting remains fragmented. For most tech companies, the decision hinges on employment contracts, which may include exclusivity clauses, confidentiality agreements, and non-compete provisions. However, many organizations—particularly those in growth phases—tend to lack robust or standardized employment contracts, often resulting in informal or loosely structured employment terms, especially when hires are made quickly through networks and referrals. The absence of clear contractual terms creates ambiguity, which can be exploited to engage in dual employment without consequence. Even when such clauses exist, enforcement remains a challenge—especially in today's environment of remote work and a growing sentiment among employees regarding the desirability of multiple 'gigs' to expand their income sources.

In such a landscape, early and accurate verification becomes critical. Organizations need to go beyond relying on contracts alone and proactively verify the identity, background, and employment history of candidates before onboarding. Technology-powered solutions are designed to do exactly that. Automating background verification can help companies verify key credentials—such as identity, past employment, and qualifications—safeguarding companies against risks like fake profiles, deepfakes, and resume misrepresentation. By ensuring that only verified, trustworthy talent is hired, such platforms strengthen the recruitment process while helping protect organizational integrity and reputation.

Alongside moonlighting, another growing concern is the increasing prevalence of counterfeit claims, documents, and certificates. This risk spans multiple sectors and is especially pronounced in fast-paced hiring environments. These falsified documents are not only inexpensive and easy to access—they can often be created within hours—making them particularly appealing to individuals with limited experience or intent to deceive.

As organizations continue to navigate the complexities of today's workforce, implementing digital background checks is no longer optional—it's essential.

Authenticating documents using advanced technologies can address this risk. Conducting multi-level checks and advanced statistical algorithms to detect forged or altered documents can help organizations make informed hiring decisions and avoid reputational and compliance risks.

Utilizing AI and ML-powered analytical insights enhance fraud detection capabilities through:

Optical Character Recognition (OCR): To extract and verify textual information from scanned documents

GST checks: Helps validate goods and services tax (GST)-related data

Personal information verification: To confirm the accuracy of personal details

Vendor authentication: Helps ensure the legitimacy of vendor information

By streamlining document verification, businesses can proactively monitor transactions, strengthen compliance, and make informed decisions with greater confidence. Building on this foundation of technology-driven risk management, companies can harness cloud-based, AI-powered platform that present disparate data points to further streamline compliance, investigations, and risk management. Leveraging advanced analytics, automation, and machine learning can enable organizations to detect issues faster, manage data efficiently, and uphold integrity. Adopting secure, scalable solutions that integrate seamlessly with existing systems can ensure that businesses stay ahead in an evolving risk landscape.

Trust and integrity

The past few years have witnessed sweeping changes in India's regulatory environment—from data privacy and ESG reporting to AI adoption and anti-corruption reforms. These shifts have fundamentally reshaped how businesses operate and increased the intensity of regulatory scrutiny. As a result, organizations are facing a surge in corporate investigations, disputes and compliance-related challenges, creating an unprecedented demand for forensic specialists, financial crime experts and risk advisory services.

As risks grow in complexity, organizations must strive to adopt sector-focused, globally scalable tech solutions to navigate risk, meet the highest integrity standards, and drive long-term value. It is important to continuously monitor the risk lifecycle to enable swift response to fraud incidents and minimize crises before they materialize. At the same time, the growing regulatory complexity is creating an urgent need for legal, compliance, and risk professionals to upskill and stay future-ready. Conducting specialized eLearning programs and developing knowledge-sharing platforms will equip future forensic, compliance, and governance professionals with practical, technology-driven insights.

Sector-focused solutions

A one-size-fits-all approach to fraud risk management can be restrictive and often inadequate. Companies need to tailor a dynamic and multipronged approach to ensure their framework is scalable and can address emerging frauds specific to the sector they operate in. Fraud risks vary significantly across sectors due to differences in operational models, regulatory environments, and threat vectors. Replicating the framework that worked for one company for the other can often undermine these nuanced vulnerabilities. Sector-specific solutions enable organizations to address the unique fraud risks they face, ensuring more precise detection, prevention and response mechanisms.

Implementing industry-specific fraud risk strategies not only strengthens compliance with relevant regulations but also enhances operational efficiency. By aligning fraud controls with sectoral workflows and compliance mandates, organizations can reduce false positives, streamline investigations, and allocate resources more effectively. This targeted approach fosters a proactive fraud mitigation culture and builds resilience against evolving threats within each industry.

Banking, financial services, and insurance (BFSI)

The BFSI sector is being increasingly plagued by sophisticated fraud schemes that exploit the digital infrastructure, regulatory gaps, and customer trust. A generic approach to fraud management cannot address the nuances of the threats faced by the BFSI sector. Instead, a tailored, sector-aware strategy is critical to building resilience and trust in an increasingly digital financial ecosystem.

In banking, scams such as the 'jumped deposit' fraud manipulate users into authorizing UPI transactions under false pretences, often by exploiting casual PIN entry habits. Increase in incidences of phishing attacks and unauthorized international transactions have prompted the Reserve Bank of India to mandate Additional Factor Authentication (AFA) and the adoption of TRAI's Mobile Number Revocation List (MNRL) technology. These measures are tailored to address the specific vulnerabilities of digital banking systems and further underscore the need for fraud controls that are not only robust but also sector specific. Banks need to leverage advanced technology to protect themselves and loyal customers against tech-savvy fraudsters and to fraud-proof their systems against similar attacks in the future.

In the financial services domain, fraudsters are leveraging social media and dormant mobile apps to pose as SEBI-registered advisors, luring investors into fake trading groups and VIP clubs. Scams like these often involve forged certificates, unverified advisory platforms, and promises of unrealistic returns. The proliferation of such fraud incidents highlights the inadequacy of generic fraud detection tools in identifying market manipulation and misinformation. Financial services companies must harness targeted surveillance mechanisms, investor verification protocols, and real-time monitoring of advisory channels to effectively mitigate fraud risks.

The insurance sector faces its own set of challenges, with fraudsters impersonating regulatory bodies and agents to sell fake policies or promise refunds on lapsed ones. Victims are often manipulated through pressure tactics and misleading documentation, with payments collected via personal UPI IDs. These scams exploit policyholder data and regulatory blind spots, making it imperative for insurers to deploy fraud detection systems that can authenticate agent identities, validate policy documents, and flag suspicious refund claims. Not only will tech intervention help protect the interests of the insurers, but it will also mitigate the risks arising from fraudulent claims that can siphon off considerable funds from the insurance company.

IT/ITES

The IT/ITES sector in India is undergoing rapid expansion, driven by the growth of Global Capability Centers (GCCs), increased demand for engineering R&D, and rising global market share. With over 126,000 new jobs expected to be added in FY25, the sector's scale and complexity are evolving swiftly. However, this growth also brings heightened exposure to fraud risks, particularly in talent acquisition and workforce integrity. The rise in short fuse hiring requests has made speed a priority, often at the expense of thorough due diligence efforts. This creates vulnerabilities that can be exploited through falsified credentials, misrepresented employment histories, and fraudulent onboarding documentation.

The hybrid work model has further complicated fraud risk management, with glaring incidences of dual employment or moonlighting emerging as significant threats. These practices not only compromise organizational confidentiality but also undermine productivity and trust. In response, leading tech firms are revising their "do not hire" lists, scrutinizing employment records from the COVID period, and cross verifying the legitimacy of previous employers. Some organizations have gone a step further by deploying background verification representatives on-site to streamline document collection and reduce insufficiencies. These measures reflect the need for tailored fraud controls that address the unique challenges of remote work, high-volume hiring, and sensitive data environments.

Given the sector's reliance on intellectual property, client trust, and global delivery models, generic fraud prevention frameworks are insufficient. IT/ITES companies require sector-specific solutions that integrate workforce analytics, real-time verification tools, and proactive risk checks. These steps will help detect anomalies in employment patterns, flag inconsistencies in documentation, and ensure compliance with evolving hiring needs. As industry continues to scale, building a resilient fraud management ecosystem tailored to its operational realities is imperative.

Pharma/medical devices

The pharma sector is highly regulated and factors such as product integrity, patient safety and compliance are paramount. Fraud in this sector can be a matter of life and death, but complex supply chains, fraudulent employment claims and stringent quality standards leave the sector vulnerable to frauds such as counterfeit drugs, falsified clinical data and misrepresentation. These risks are amplified due to globalized operations, making traceability much more difficult.

The rise of digital health platforms and telemedicine has introduced new fraud risks such as data breaches, identity theft, and manipulation of electronic health records. Medical device manufacturers and pharma companies must also deal with risks related to IP theft, personal data harvesting, and unauthorized product modifications. Generic cybersecurity frameworks are insufficient to address these threats. Instead, tailored solutions that integrate device-level authentication, secure data transmission protocols, and compliance with health data privacy regulations like the HIPAA or India's DPDP Act, are critical for fraud prevention in this sector.

As the sector continues to innovate and expand, building a resilient fraud risk management ecosystem that reflects its unique operational and ethical challenges is a must. Along with industry-specific governance mechanisms– such as transparent audit trails, third-party validation of research, and automated monitoring of promotional content– sector-specific fraud controls must also be implemented to safeguard public trust in the healthcare domain.

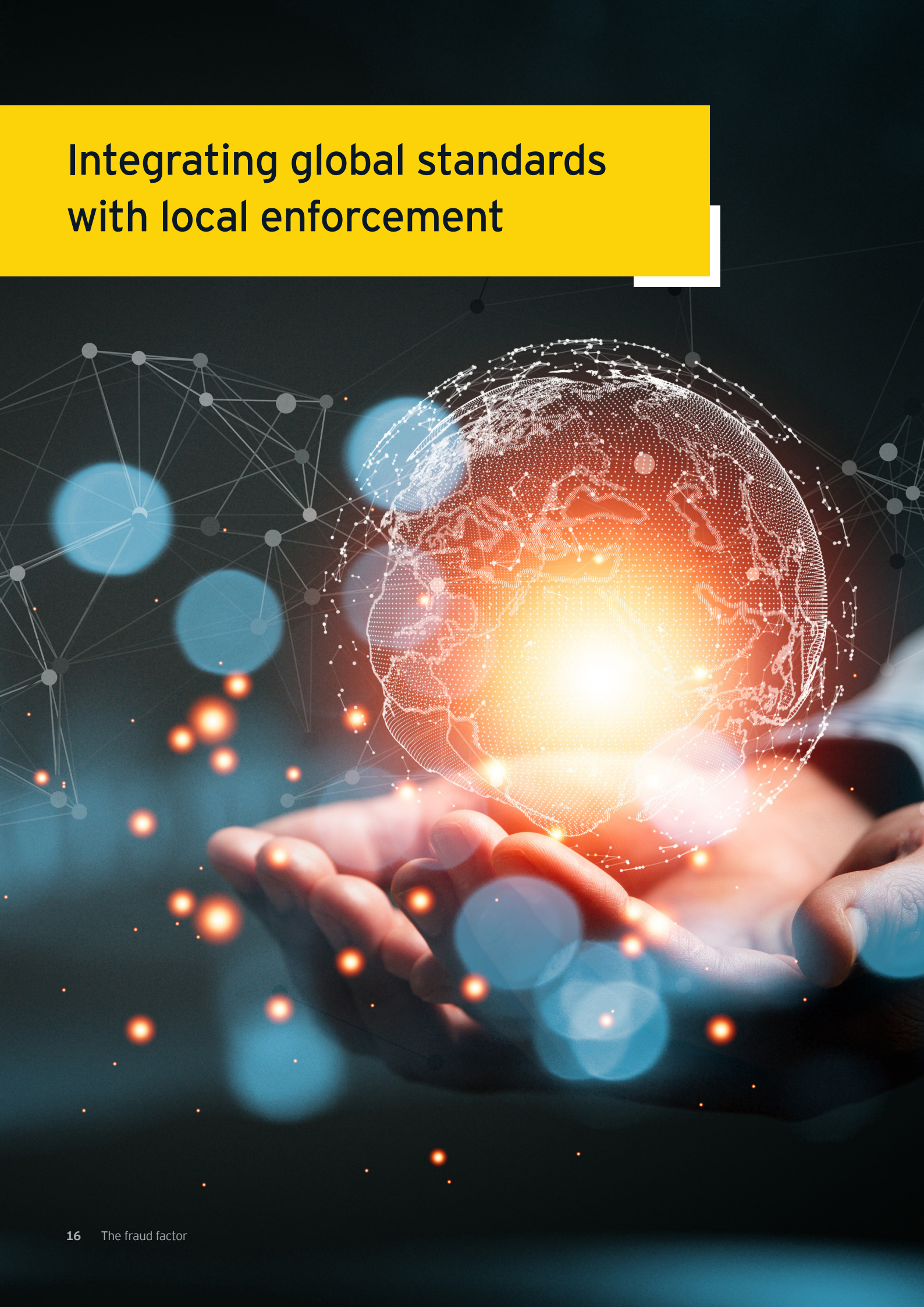
FMCG

With high-volume transactions, rapid inventory turnover and widespread distribution networks, the FMCG sector is highly susceptible to frauds such as counterfeit products and supply chain manipulation. The proliferation of fake goods not only erodes brand equity but also poses health and safety risks to consumers. Sector-specific fraud controls such as tamper-proof packaging, QR code-based product authentication, and distributor-level verification systems are essential to ensure product authenticity and traceability.

Fragmented retail ecosystems and limited visibility into last-mile operations further complicate the nature of FMCG operations, providing an impetus for fraudsters to introduce counterfeit products at several levels of the operation. Generic fraud detection tools may fail to capture these instances. FMCG companies require tailored analytics platforms that can monitor transactional anomalies, validate claims, and detect irregularities in inventory movement across geographies and channels.

Additionally, managing vendor fraud, especially in procurement and logistics, is one of the main concerns that plague the sector. False billing, duplicate payments, and collusion between internal and external stakeholders can lead to significant financial losses. To mitigate these risks, FMCG firms must implement sector-specific controls such as vendor onboarding verification, automated reconciliation systems, and AI-driven procurement audits. As consumer expectations and regulatory scrutiny increase, a customized fraud risk management approach is vital to maintain brand reputation, ensure operational integrity, and prevent financial losses.

Integrating global standards with local enforcement



The imperative for harmonized global regulatory standards to combat fraud effectively

The global regulatory landscape is marked by diverse and evolving approaches, shaped by regional, political, economic and social contexts. In the US, a trend toward deregulation, especially in the environmental sector—has emerged, driven by economic growth objectives. While this may reduce operational burdens for businesses, it also raises concerns about long-term sustainability and public accountability, which are critical in fraud prevention frameworks. Conversely, the UK has adopted a more stringent regulatory stance, particularly in areas like data protection and environmental compliance. In the Asia-Pacific region, regulatory strategies vary widely. With China implementing the Cybersecurity Law, which mandates data localization and government oversight, and India introducing the Digital Personal Data Protection Act—demonstrating their commitment towards building a resilient economy. Meanwhile, smaller economies in the region are liberalizing regulations to attract foreign investment, which can create vulnerabilities if not balanced with adequate safeguards.

Fraud schemes have become increasingly sophisticated, often operating across multiple jurisdictions to exploit regulatory loopholes and language discrepancies. Fraudsters harness these gaps to move illicit funds, manipulate financial systems and evade detection. Without a unified approach, efforts to combat fraud will remain fragmented, reactive and limited in scope—making it difficult to track and prosecute offenders effectively. Uniformity in global regulatory standards offers a solution by creating a consistent framework for identifying, reporting and addressing fraudulent activities. Such standards can enable countries to share intelligence more efficiently, align enforcement practices and reduce fraud risk.

Moreover, harmonization of standards fosters trust among international stakeholders, governments, financial institutions, and businesses—by ensuring that everyone operates under the same expectations and accountability measures.

Strategies for scaling localized anti-fraud initiatives to meet international compliance demands

While global standards will boost anti-fraud efforts, companies can start scaling up their fraud risk management to be fully compliant. To effectively scale localized anti-fraud initiatives, organizations must first develop a unified compliance framework that accommodates regional regulatory nuances. Working towards building transparency, accountability, and data integrity into every function is the first step towards creating a framework that can live up to the regulatory expectations in most jurisdictions. Achieving consistency in fraud prevention efforts while maintaining agility can help companies prepare themselves to adapt to evolving laws.

Automating compliance with AI-driven analytics, blockchain, and centralized compliance platforms plays a pivotal role in scaling anti-fraud initiatives globally. These tools can facilitate real-time monitoring, automated reporting, and predictive risk assessments across multiple jurisdictions—presenting key insights at-a-glance for informed decision-making. Integrating localized data sources into a global compliance dashboard allows organizations to detect anomalies and fraud patterns that may be overlooked while working in silos.

Additionally, investing in capacity building through training programs, multilingual compliance resources and regional expertise empowers local teams to implement global strategies effectively. This collaborative approach not only strengthens fraud resilience but also enhances trust and transparency across international operations.

Building a cohesive ecosystem that integrates global and local efforts for comprehensive fraud mitigation

Organizations must invest in understanding associated risks and regulatory landscapes to tailor global anti-fraud strategies that also address local needs. This alignment ensures that fraud prevention efforts are both compliant and culturally sensitive, reducing friction in implementation. Technology plays a central role in integrating global and local anti-fraud efforts to allow seamless data exchange between jurisdictions and track cross-border fraud activities. Establishing shared intelligence networks such as fraud registries, real-time alert systems, and collaborative analytics platforms can empower stakeholders to detect and respond to threats more effectively. These systems can be further customized to maintain data sovereignty while enabling secure collaboration across borders.

Adopting innovative fraud detection tools and practices can enrich global strategies with diverse perspectives and solutions. Fostering a culture of trust and transparency between global and local entities will ensure cooperation, helping to present a unified front against increasingly sophisticated fraud schemes.

EY Key contributors

EY Leadership

Arpinder Singh
India & Emerging Markets Leader,
EY Forensic & Integrity Services
arpinder.singh@in.ey.com

Sandeep Baldava
Partner
EY Forensic & Integrity Services
sandeep.baldava@in.ey.com

Sectors

Vikram Babbar
Partner
EY Forensic & Integrity Services
vikram.babbar@in.ey.com

Rajiv Joshi
Partner
EY Forensic & Integrity Services
rajiv.joshi@in.ey.com

Anurag Kashyap
Partner
EY Forensic & Integrity Services
anurag.kashyap@in.ey.com

Tech solutions

Vivek Aggarwal
Partner
EY Forensic & Integrity Services
vivek.aggarwal@in.ey.com

Harshavardhan Godugula
Partner
EY Forensic & Integrity Services
harshavardhan.g@in.ey.com

Amit Mishra
Partner
EY Forensic & Integrity Services
amit3.mishra@in.ey.com

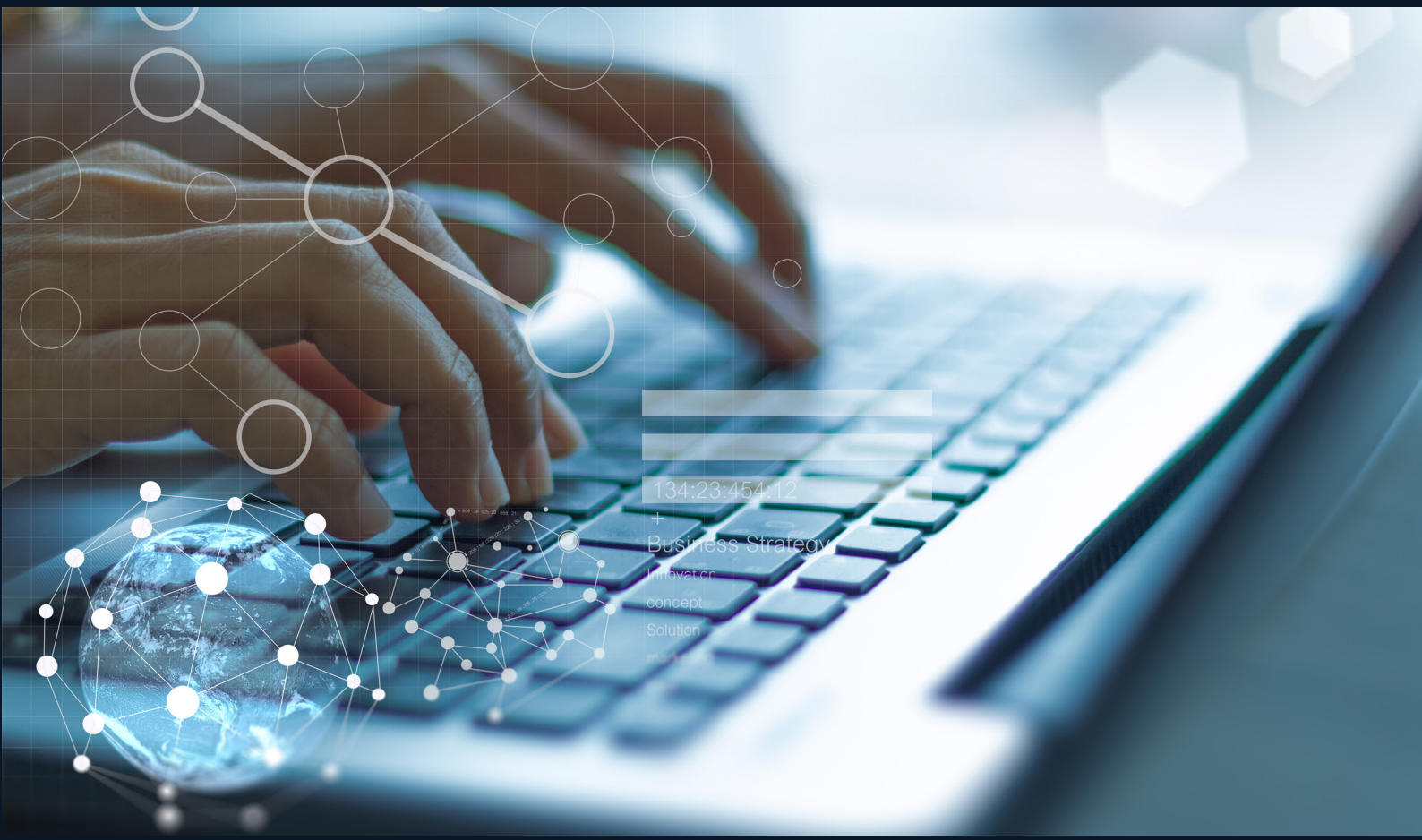
Swapnil Sule
Director
EY Forensic & Integrity Services
swapnil.sule1@in.ey.com

FICCI Key contributors

Sumeet Gupta
Deputy Secretary General
sumeet.gupta@ficci.com

Gaurav Gaur
Additional Director
gaurav.gaur@ficci.com

Aastha Gupta
Senior Assistant Director
aastha.gupta@ficci.com



Ernst & Young LLP

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYIN2508-007
ED None

ey.com/en_in

@EY_India EY EY India EY Careers India

@ey_indiacareers

FICCI

Established in 1927, Federation of Indian Chambers of Commerce and Industry (FICCI) is the largest and oldest apex business organisation in India. Mahatma Gandhi addressed FICCI's 4th AGM in 1931. Our 96th AGM was held in December 2023. With our rich legacy, FICCI would play an even greater role as India emergence as the 3rd largest economy.

FICCI works with its key stakeholders to foster active engagement and dialogue with decision makers, to support steps that are good for commerce and industry.

As a member-led and member-driven organisation, FICCI represents ov er 2,50,000 companies across all segments of economy including public, private and multinationals. The diverse membership base of FICCI across all Indian states includes both direct and indirect members through its 300 affiliated regional and state level industry associations. FICCI has a large international presence via partner agreements with 250 national business associations in over 100 countries.

www.ficci.in ficciindia ficci_india ficci_india ficci blog.ficci.com