



MGC
GLOBAL RISK ADVISORY LLP

FRAUD MITIGATION

THROUGH THE LENS OF
CORPORATE GOVERNANCE

Disclaimer

This report has been prepared by MGC Global Risk Advisory LLP, in collaboration with the India Leadership Council by The Times Group. The contents herein are intended solely for informational purposes and do not constitute professional advice, endorsement, or recommendation. While every effort has been made to ensure the accuracy, reliability, and completeness of the information presented, MGC Global Risk Advisory LLP and the India Leadership Council by The Times Group expressly disclaim any and all liability arising from reliance on the report's contents. The views and analyses expressed are based on data and insights available at the time of publication and are subject to change without notice. Readers are advised to exercise their own judgment and seek independent professional counsel before making any decisions based on the information provided under this report.

Fraud mitigation through the lens of corporate governance

The new fraud economy

Organizations are increasingly being forced to view fraud through a different lens. The conversation is shifting away from the aftermath of fraud and towards the conditions that allow it to occur in the first place. Who can commit fraud, how fast it moves and how long it takes an organization to detect it, are becoming leadership questions rather than investigative ones. Three structural shifts are heightening the concern around fraud. First, AI has lowered the cost, skill and time required to execute fraud at scale. Second, regulators have raised the cost of governance failure,

including through regimes such as the UK's Failure to Prevent Fraud offence. Third, the fraud perimeter has expanded beyond the organization's own walls to vendors, platforms, partners, agents and other third parties that leadership may not directly control but must still oversee.

CFEs expect that organizations **LOSE**

5% of revenue to **FRAUD** each year.

Source: [ACFE \(2026\)](#).

Are Boards and CEOs ready to tackle the evolving nature of fraud? Are their governance systems equipped to detect emerging fraud risks before they become material events? These are some of the questions which will define the quality of governance and resilience in the decade ahead.



Why governance fails before F(raud) happens

Most boards believe their organizations have adequate fraud controls. Most are right. The controls exist. The problem is that fraud does not enter through controls. It enters through the gaps between them.

The *ACFE Occupational Fraud 2026: Report to the Nations (2026)* tells us the median fraud runs for 12 months before detection. That means for every fraud that surfaces in an organization, the governance breakdown that enabled it began a year earlier - while the audit committee was meeting, while the internal controls were operating, while the risk reports were being filed.

Where fraud actually begins

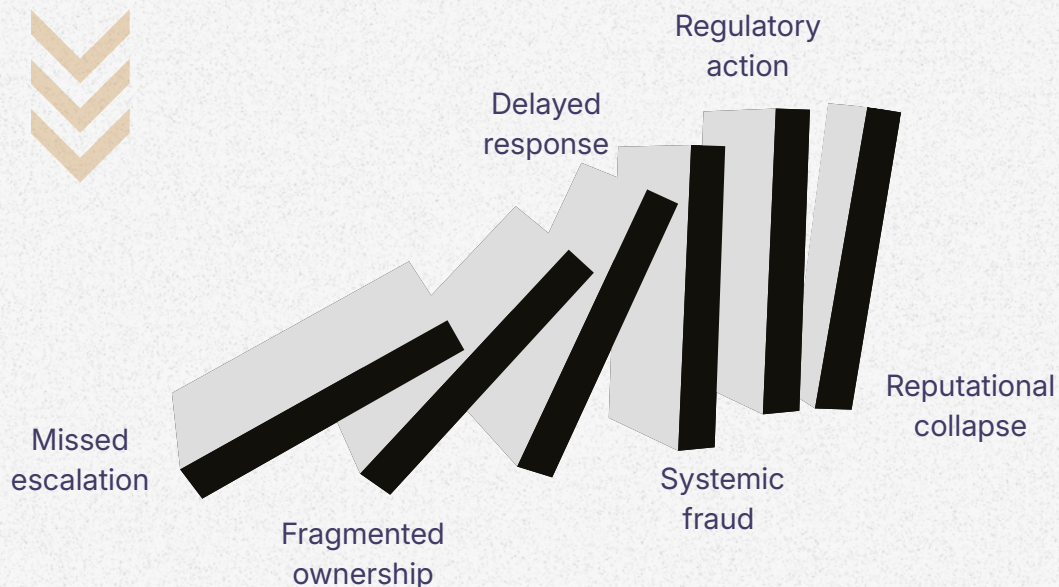


Fig. 1: The governance multiplier effect

Cases such as Satyam Scandal, Yes Bank and DHFL all point to the same conclusion: major fraud and governance failures rarely begin with a missing control; they begin when information flow, decision rights and independent challenge break down. In each case, warning signals existed long before the crises became visible, but boards did not receive, test or act on them with sufficient independence and urgency.



Satyam
Scandal, India

- **Detection method:** Whistleblower/ external investigation
- **Duration before detection:** ~ 7 years
- **Prior signal:** Internal concerns existed; no functioning escalation path to Board



Yes Bank, India

- **Detection method:** RBI inspection / external regulatory
- **Duration before detection:** Multiple years
- **Prior signal:** Credit decision inconsistent with risk policy; Board did not independently scrutinize



DHFL, India

- **Detection method:** Investigation journalism / external audit
- **Duration before detection:** ~ 3 years
- **Prior signal:** Related-party transaction embedded in financials; audit committee did not independently test

Increasingly, the organizations that detect, prevent and respond to fraud are unlikely to be those with the most controls, but those with the shortest distance between emerging risk and executive action.

Who owns fraud risk?

If an organization cannot answer this question in ten seconds, the organization has already failed its first governance test.

Distributing fraud across risk, compliance, finance and operations undermines accountability. When fraud surfaces, the question of who was responsible for preventing it, goes unanswered. Shared ownership frequently translates into no clear ownership at all.

Singular ownership, along with joint executive stewardship is the first step to tackle fraud risk. The CEO must own fraud risk, not as a title, but as the architect of how authority, escalation and consequence are wired into the operating model.

The CFO and CRO must act as joint stewards because fraud thrives when financial performance is discussed without reference to risk and when risk is discussed without reference to commercial consequences. Ultimately, the Board's role is not to own fraud, but to ensure ownership is explicit, measurable and tested.

The new fraud frontier: What Boards and CEOs must now govern

Historically, fraud was perceived as an operational risk. However, over the years, it has taken centre stage through becoming an enterprise-wide risk, with its ability to enter into an organization through different forms. Four forces are defining the fraud environment in 2026:

1. AI: The capability equalizer

AI is evolving and accelerating at a pace which most Boards and CEOs are unable to comprehend. AI-generated invoices are bypassing the standard three-way matching. The PO reference is valid, the vendor record exists - the document looks correct. Traditional controls may not identify the anomaly. Deepfake audios and videos are used to authorize wire transfers. CFOs are receiving calls and video instructions from individuals who look and sound like their CEO.



Source: PIB, 2026

KEY STATISTIC

Over

₹52,000 crore

has been lost to cyber frauds in India over the last five years

Justifiably, The World Economic Forum (2026) ranks AI driven misinformation and adverse AI outcomes among the top global risks of the coming decade. While the barrier to committing sophisticated fraud has collapsed, the barrier to detecting it has not kept pace.

Such instances point to the reality of AI: it has permeated an organization’s fraud surface, decision workflows and external ecosystem, making the threat immediate rather than theoretical.



What should CEOs do?

CEOs must realize that AI is double-edged sword. While automation is necessary, it also opens the door to challenges which organizations may not foresee.

CEOs need accountable human decision-makers who can challenge automated outputs, escalate anomalies and stop high-risk activity before it becomes a loss. The Reserve Bank of India’s (2026) proposed ‘kill switch’ mechanism is guided through the same principle: AI systems require human override when model risks arise.

Without human judgement, the organization’s fraud strategy will remain reactive, fragmented and dangerously slower than the threats it is expected to contain.

2) Ecosystem exposure: You are only as clean as your supply chain

Organizations which outsource execution, inherit risks they do not directly control. Third-party fraud, supply chain misrepresentation and vendor collusion now sit outside the organization's internal controls framework, but squarely inside its regulatory and legal exposure.

Across Asia-Pacific, procurement and third-party fraud are the most significant fraud risks faced by organizations (ACCA Global, 2025). The risk does not sit uniformly across the vendor relationship. It spikes at two points: onboarding, where due diligence gaps and undisclosed ownerships enter; and execution, where invoice fraud, overbilling and phantom deliverables emerge once scrutiny has relaxed.



Stale due diligence is a specific risk that leadership teams consistently underestimate. A vendor that was checked at onboarding three years ago may have changed ownership, a related-party connection to an employee may have emerged, or the vendor may have been flagged in another investigation. If due diligence stops after onboarding, governance failure begins and the vendor remains on the approved list while invoices continue to be processed.

Such inherited risks will test CEOs on their assumptions about the relationships on which their business depends. Re-verification of high value vendors, therefore, becomes a strategic priority.

3) ESG: The next material misrepresentation risk

A study by the Advertising Standards Council of India found that 79% of environmental "green" claims made by organizations were exaggerated or misleading. (Mongabay, 2024). When boards sign off on ESG data that they cannot independently verify, they are not managing a reporting obligation, instead, they are creating the conditions for material misrepresentation. ESG is no longer a disclosure exercise. It is a fraud surface.

SEBI's BRSR framework has made ESG-data a current legal exposure, not something to act on, in the future. With the extension of BRSR Core for the value chain (while currently voluntary), CEOs will have to face a more demanding reality: how their value chain ESG-data has been verified, challenged and governed.

The current and future environment will not test whether ESG disclosures are compliant, but whether they are true.

4) Geopolitical instability and insider risk

Geopolitical instability does not create fraud risk in isolation; it weakens the governance conditions that contain it. Supply disruption compresses due diligence, margin pressure increases tolerance for exceptions and shifting trade relationships create new sanctions and counterparty exposures.

The more uncomfortable risk for Boards is internal. ACFE (2026) finds that frauds committed by owners and executives result in median losses of US\$475,000 and remain undetected for a median period of 23 months, far exceeding employee-level fraud.

The governance issue is clear: the individuals best placed to override controls are often those under the greatest commercial pressure. Since no internal control sits above senior authority, this risk can only be tested and challenged at Board level.

What does inadequate governance actually cost?

Median losses by fraud type

The highest-value frauds take the longest to detect and are least likely to be caught by internal audit.

	 MEDIAN LOSS (USD)	 MEDIAN DETECTION TIME	 PRIMARY DETECTION METHOD
01	FINANCIAL STATEMENT FRAUD \$766K	24 MONTHS 	 External audit / tip – rarely internal audit
02	SENIOR MANAGEMENT FRAUD \$475K	24 MONTHS 	 Tip – board oversight rarely surfaces it independently
03	CORRUPTION / BRIBERY \$200K	18 MONTHS 	 Tip or external investigation
04	PROCUREMENT FRAUD \$130K	12 MONTHS 	 Internal audit / account reconciliation
05	ASSET MISAPPROPRIATION \$120K	12 MONTHS 	 Internal audit / tip

Source: ACFE (2026)

The five questions every CEO must ask

01 Where does fraud accountability sit when no one is looking?

If accountability only exists inside committees, dashboards or policy frameworks, it does not exist in practice. The CEO must be able to point to a single accountable executive whose authority is real under pressure, including when the issue involves performance trade-offs, senior leadership conduct or commercial inconvenience. The governance test is not whether ownership is defined in documents, but whether it survives ambiguity, conflict and escalation fatigue.

02 What is the shortest path from suspicion to intervention?

Most organizations design reporting structures; few design time to action. Fraud resilience depends on whether signals can move from detection points (employee, vendor, system, auditor) to decision authority without distortion, delay or dilution. Where escalation depends on hierarchy, interpretation layers or functional mediation, fraud does not get stopped earlier, it gets formalized later. The CEO's strategic question is: how many handoffs exist between signal and stop authority?

03 Where does your operating model quietly trade integrity for performance?

Fraud risk rarely emerges from absence of controls. It emerges from conflict between incentives and oversight. This includes targets that reward outcomes without validating process integrity, procurement pressure that compresses due diligence and revenue expectations that normalize exceptions. The governance failure is not in the incentive itself, but in the absence of an explicit mechanism that surfaces when performance pressure is beginning to override control discipline. If no such mechanism exists, the system is implicitly choosing performance over integrity and only discovers the cost retrospectively.



04 Which parts of your ecosystem are effectively beyond your governance visibility?

Modern fraud does not respect organizational boundaries. It propagates through vendors, subcontractors, platforms and intermediaries that are operationally embedded but governance-light. The strategic risk is not third-party fraud itself, but assumed equivalence of control standards across the ecosystem. Most organizations perform onboarding diligence; far fewer maintain continuous identity, ownership and behaviour verification of high-impact partners. The CEO-level question is not “do we vet vendors?” but: where in our value chain do we no longer meaningfully see risk change over time?

05 What is the organization not telling itself about fraud risk?

Every governance system develops blind spots, not from absence of data, but from over-reliance on internal interpretation of that data. Where fraud intelligence is fully mediated through finance, risk, compliance or internal audit narratives, CEOs receive processed reality, not raw signal diversity. Resilience depends on whether leadership has access to at least one independent lens on fraud emergence that is structurally separated from the functions responsible for reporting on it. The question is not whether assurance exists, but whether it is sufficiently independent to contradict the internal consensus.



CEO action – for the next 120 days

1. Collapse ambiguity in accountability design (0-30 Days)

Assign a single executive accountable for fraud risk architecture – not monitoring, not reporting, but system design and escalation integrity.

The output should be explicit: decision rights, escalation thresholds and Board visibility triggers. If this cannot be clearly mapped, accountability is still distributed rather than assigned.

2. Stress-test escalation under real organizational pressure (30-60 Days)

Simulate fraud scenarios where normal governance assumptions fail:

- involvement of senior leadership
- compromised whistleblower confidence
- commercial pressure to delay disclosure
- control override by authority, not error

The objective is not control validation. It is to observe where governance slows down, gets filtered, or becomes socially constrained.

3. Audit incentive-pressure interactions, not just incentives (60-90 Days)

Review where performance systems interact with control systems in practice:

- where exceptions are routinely normalized
- where verification is bypassed for speed
- where escalation is discouraged implicitly

The output should identify “pressure corridors” – points where behaviour predictably deviates under target stress.

4. Map governance opacity across the value chain (90-120 Days)

Identify where the organization relies on trust without verification across:

- critical vendors
- outsourced execution layers
- high-volume transaction intermediaries

The key output is not vendor risk scoring, but identification of areas where risk change is not continuously observable.

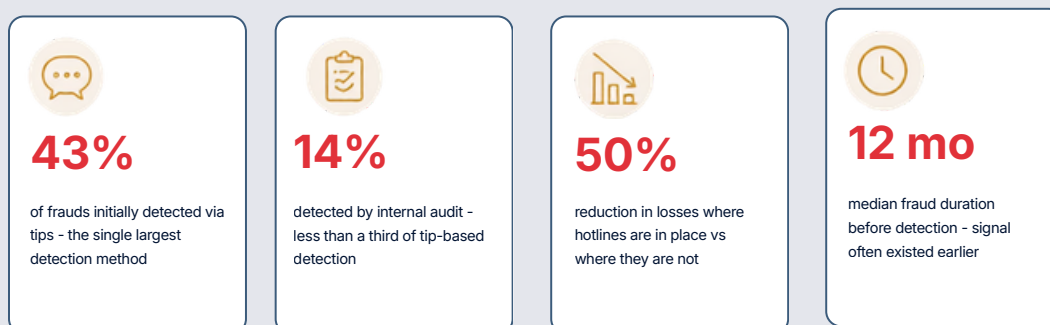
5. Build a second lens of fraud intelligence (From Day 0, ongoing)

Establish an independent channel of fraud insight that is not structurally dependent on the functions being assessed.

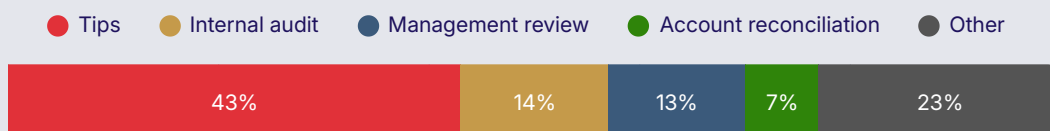
This is not additional reporting. It is *architectural independence* - ensuring that the CEO and Board are not solely reliant on internally produced narratives of risk.

What whistleblowers actually surface and what happens when they don't

Tips are the primary fraud detection method globally. The question is not whether your mechanism exists. It is whether people trust it enough to use it.



How frauds are initially detected?



Source: [ACFE \(2026\)](#)

Conclusion: Governance as the strongest antidote to fraud

As the new fraud frontier expands the attack surface, organizations can no longer rely on controls designed for a different era. The fraud landscape of 2026 will test the ability of organizations to adapt their governance frameworks, accordingly.

The governance systems of today must be capable of identifying vulnerabilities, escalating warning signals and intervening before risks materialize into enterprise-wide failures and losses. Fraud resilience will therefore emerge as the defining characteristic of governance maturity for the decade ahead. It will not be a compliance investment, but rather the infrastructure of trust on which sustainable organizational performance depends. The Boards and CEOs who treat it that way will be better positioned when the environment, as it will, gets harder.