

Prevention of Corporate Frauds – Magnificent 7 Ideas

A thought leadership perspective for global auditors, board members, and regulators



Parveen Kumar
National Head-Assurance
ASA & Associates LLP

Corporate Frauds

Corporate fraud may be defined as a ‘**deliberate**’ misrepresentation or concealment of material facts by an individual for personal gain or interests of any organisation at the expense of its stakeholders, which may include investors, creditors, employees or the public at large. Corporate fraud is different from stealing and small theft because it is generally premeditated, systemic, and executed by those entrusted with power.

According to a study on occupational fraud¹ organisations globally are estimated to lose 5% of their annual revenues to fraud each year. As per this recent study, which is based on analysis of 2402 cases across 143 countries, an estimated amount of loss was exceeding USD 3.4 billion. These are only which were detected and reported, many more might have been undetected. Within Corporate fraud, Financial Statement Fraud is significantly different from Asset Misappropriation. The paradox is stark and worth pondering on. While financial statement fraud accounts for only 5% of cases, it causes median losses more than six times greater than that in case of asset misappropriation. It is the tip of the iceberg that sinks ships. Boards, audit committees, auditors and regulators must recognise that frequency and severity are inversely correlated and calibrate their attention accordingly. Let us have a look at a couple of historical landmark cases to set the context.

Enron Corporation (USA, 2001)² was once the largest company in the United States, acknowledged fraudulent financial reporting spanning five years, during which it concealed massive debts and losses using off-balance sheet special purpose vehicles. When the scheme collapsed, Enron filed for one of the largest corporate bankruptcy in US history. Five years of financial statements signed off by its auditor Arthur Andersen had to be restated. Shareholders lost billions virtually overnight, and thousands of employees lost their retirement savings.

Wirecard AG (Germany, 2020)³ was once a darling of European fintech, collapsed after it was revealed that a huge amount of cash, that was appearing in the financial statement, was actually missing. The fraud had been orchestrated for years, combining false accounting with inflated revenue from fictitious clients. Its long-serving auditor EY refused to sign the accounts because it couldn't verify the existence of €1.9bn of assets. Wirecard filed for insolvency on 25 June 2020, wiping out nearly EUR 25 billion in market capitalisation.

Magnificent 7 Ideas

Prevention is better than cure, and timely detection is superior to loss recovery. Drawing on three and a half decades of audit and consulting practice, in my experience, the following ideas represent not a theoretical checklist but a battle tested, actionable agenda for boards, executives, and professionals who are serious about making their organisations fraud resistant. Challenges are inevitable but there are tricks to manage them. We will discuss these challenges alongside.

Anonymous Reporting and Action

The data in report we discussed above is unambiguous. Tips account for 43% of fraud detection, and organisations with a reporting hotline suffer 50% lower fraud losses. Yet many organisations treat whistleblower policies and procedures as a compliance box tick rather than a genuine intelligence asset. An effective mechanism must be truly anonymous, operated by preferably an independent third party, accessible 24/7 across multiple channels (phone, web, email), and actively promoted at all organisational levels including external stakeholders like vendors and customers.

Organisations generally hush up fraud to protect reputations. Every substantiated fraud must be rigorously investigated, reported to law enforcement where required, and culprit should be prosecuted to the fullest extent possible.

On action, practicality is taken as shield. The argument that litigation is expensive and time consuming besides recoveries are minimal overshadow actions. Nevertheless, the deterrent value of consistent enforcement far exceeds its direct cost. Regulatory referrals and industry debarment are levers that organisations should use without hesitation, may be as example.

Power House called Audit Committee

Audit committees that meet perfunctorily and work like a rubber stamp of management's narrative are a governance illusion. An effective audit committee must comprise financially literate, genuinely ‘independent’ directors with the mandate, the skill, and the willingness to probe, challenge, and escalate. It should have a direct, unmediated reporting line from internal auditor and external auditor and must regularly meet with both of these without management present. The audit committee's independence is the one of the most important governance safeguards against top-management fraud.

Practically, in most of the promoter driven entities, audit committees are frequently populated with associates of the controlling shareholder, rarely rendering meaningful oversight. While regulators try to enforce substantive independence, the professionals could also play an important role here.

Fraud Risk Assessment Calendar

A frequent formal fraud risk assessment is required to identify vulnerability, which might be due to opportunity or gap in controls. This must be conducted at least annually if not half yearly in high risk environments. This assessment could be owned by the board, not delegated entirely to management, given that management level fraud is precisely where the greatest loss occur.

It is advisable to include 'unannounced' forensic reviews of high risk areas. These can be conducted by specialists with forensic skills can intercept emerging schemes before they scale. The element of surprise is critical; scheduled reviews give time to perpetrators.

Quite a few corners in corporate world treat fraud risk assessment as an afterthought or a periodic audit exercise. Cost and the perception that forensic reviews imply distrust of management deter many boards. The counter-argument is straightforward. The cost of a forensic review is trivially small compared to the potential cost of an undetected fraud.

Having said that, a regular fraud risk assessment must be a living process embedded in strategic planning, budgeting cycles, and change in business model, geography, or leadership.

Avoid Management Override

The Auditing standards requires external auditors to identify **management override of controls** as one of the fraud risk in almost every statutory audit. Controls designed only to constrain operational staff leave a dangerous vacuum at the top. Specific measures could include requirement of dual authorisation for all material journal entries besides mandatory board level approval for any accounting policy changes. Similarly, how about having independent review of all related party transactions and segregation of duties that genuinely separates initiation, approval, and recording functions even at the highest level.

Tone at the top is not a slogan. When leaders are seen to cut ethical corners, manipulate metrics to meet targets, or retaliate against bearers of bad news, they create a culture in which fraud flourishes. Codes of conduct must be lived, not laminated.

Executives resist such controls perceiving these as questioning their integrity. The framing shift and smart narrative can be game changer, for example robust controls protect honest executives from false accusation as much as they deter dishonest ones.

Data Analytics and Continuous Monitoring

Artificial intelligence, machine learning, and advanced data analytics now makes it possible to monitor 100% of transactions in real time rather than checking a sample. Anomaly detection algorithms can flag unusual journal entries, duplicate payments, vendor master data changes just before payment runs besides revenue recognition patterns that deviate from historical norms. Organisations that invest in continuous monitoring shift the paradigm from periodic detection to real time prevention.

Implementation requires data infrastructure investment and specialised skills that many organisations lack. A practical starting point could be to deploy analytics on the high risk transaction streams (journal entries, related party transactions, vendor payments, expense claims).

Mandatory Job Rotation

Prolonged, unchecked tenure in a single role is a fraud incubator. Mandatory job rotation and compulsory annual leave (may be at least two consecutive weeks) are time-tested fraud prevention tools. Many frauds are discovered precisely when a perpetrator is on leave and a replacement uncovers the irregularity.

Operational disruption and the perceived cost of knowledge transfer often cause organisations to defer rotation indefinitely. Boards must mandate it as a non-negotiable governance standard.

Background Verification

Generally fraud perpetrators will have a prior history of dishonesty. Pre employment background verification including criminal record checks, reference verification, qualifications validation, and credit history review for financially sensitive roles must be mandatory, not discretionary. Verification will be crucial to lateral hires besides promotions at senior levels, where the stakes are highest. Periodic re screening of employees in sensitive roles is an emerging best practice.

Privacy laws vary across jurisdictions and can constrain the scope of background checks. Organisations must navigate local legal requirements while designing the most comprehensive screening permissible.

Auditor - The Last Line of Conscience

Corporate frauds are not aberration. These are human phenomenon that no regulation, technology, or governance framework can ever fully eliminate. But the evidence is clear. Organisations that invest seriously in prevention, detection, and consequence management suffer significantly lower losses and recover faster.

For auditors, the profession demands more than technical competence and professional skepticism. It requires the courage to question, the independence to stand apart, and the integrity to speak uncomfortable truths. The Enron

auditors signed off. The Wirecard auditors signed off. We, as a professional, must ensure we never become the last signature before the collapse.

The magnificent 7 ideas presented here are not exhaustive and no two organisations face identical fraud risks. Whether you are an auditor, board member, regulator, or promoter, the point is to take these ideas as a starting point for honest self-assessment and decisive action. The cost of complacency has never been higher.

The author is a Chartered Accountant and practicing auditor with over 35 years of professional experience.

¹ <https://www.acfe.com/-/media/files/acfe/pdfs/rtn/2026/2026-report-to-the-nations.pdf>

² <https://harbert.auburn.edu/binaries/documents/center-for-ethical-organizational-cultures/cases/arthur-anderson.pdf>

³ <https://www.applied-corporate-governance.com/editors-picks/wirecard-case-study/>