Deloitte.

#letstalkfraud
FAQs on tackling corporate fraud

Forensic

#letstalkfraud

FAQs on tackling corporate fraud

Q 1. Is there any special provision/regulation that deals with fraud in India?

The Companies Act, 2013 has specific provisions relating to fraud prevention and reporting. The Companies Act, 2013 explicitly defines fraud, includes severe penalties for violation, places greater accountability on Senior Management/the Board to ensure that sufficient care is taken to prevent and detect fraud (and other irregularities), provides statutory recognition to the Serious Fraud Investigative Office, introduces provisions relating to class action lawsuits, makes the establishment of a vigil mechanism mandatory for listed companies; to name a few.

Some other regulations that include provisions on fraud are:

- Indian Contract Act, 1872
- Prevention of Corruption Act, 1988
- Clause 49 of the Listing Agreement
- Indian Penal Code, 1860
- Prevention of Money Laundering Act, 2002

Q 2. What is the legal provision on the responsibility/impact on the Director and Management, if any fraud is identified?

Under the Companies Act, 2013, the primary responsibility to establish adequate internal controls to prevent and detect fraud and errors lies with the management of the entity. In the case of a company, the Board of Directors is required to state (as a part of the directors' responsibility statement in the Board's report to the shareholders) whether they:

- Had taken proper and sufficient care for safeguarding the assets of the company and for preventing and detecting fraud and other irregularities;
- Had laid down internal financial controls to be followed by the company and that such internal financial controls were adequate and operating effectively.

Under the amendments of the Companies Act 2013, the Board or Director's report is required to include a disclosure of frauds or the possibility of frauds.

Q 3. Can frauds be detected using Data Analytics/Tools? Is there any particular software or algorithm(s) that can be built to detect fraud?

Yes, they can. However, effective detection is possible only when data is gathered and stored appropriately. In our experience, most organizations face a challenge in this area as the prevailing data quality is below average to yield significant outcomes.

Organizations that do gather and store data appropriately can run data analytics routines on this data to detect patterns, discrepancies, and anomalies. Further investigation into these can reveal potential frauds. It must be noted that data analytics routines and tools need to be customized significantly to the organization's processes to yield relevant outcomes. Off the shelf tools with minimum customization may not yield the necessary results.

Q 4. What kind of controls or matrix would you suggest for early fraud detection or to mitigate fraud risks?

Certain areas that can help improve an organization's preparedness to prevent, detect, and respond to fraud are:

- Having an enforceable code of conduct
- Undertaking a fraud risk assessments (of key processes) on a regular basis
- Conducting a periodic due diligence exercise on vendors/third parties
- Continuous monitoring of transactions to detect irregularities
- Drafting and operationalizing a fraud response plan

Q 5. In a situation where the Management ignores red flags raised (of potential fraud), or takes poor/no action on critical audit findings, what should the Internal Audit (IA) team do?

In a case where the Internal Audit team becomes aware of a fraud/potential fraud incident, it is wise to report the matter to the Board or Audit Committee so that they can take further action, possibly carrying out a detailed investigation. In a scenario where the management continues to ignore concerns, the IA team can notify the statutory auditors of the organization, who have a fiduciary duty to respond, under the notification released by the MCA in December 2015, pertaining to reporting fraud. For further details on how auditors should report fraud, please read this document titled 'Reporting of frauds by the Auditor, 5 Considerations'.

Q 6. A number of organizations today rely on an outsourcing model to reduce costs. How can this be monitored and supervised to mitigate fraud?

Counter party fraud risks are a growing area of concern. In our experience, the following steps can be taken to help minimize such fraud risks.

- Conducting a thorough due diligence of the service provider's references, management, financial viability, technical capabilities etc.
- Having a written agreement/contract in place that clearly articulates the expectations and responsibilities of both sides
- Ensuring that the outsourced services provider has adequate compliance systems and security controls in place to prevent and detect fraud–these should be monitored on a regular basis and a status report may be provided to the client on a need basis
- Having a clearly defined comprehensive agreement for the transition, operational and termination phases.

Q 7. What are some of the examples of Supply Chain Fraud?

Some of the common manifestations of supply chain fraud are:

- **Leakage in the supply chain** – These could include theft of unfinished products/ packaging material; theft of inventory and misreporting scrap generated; collusion with scrap vendors and leakage of product/packaging material scrap to counterfeiters; unauthorized sale of stock to B2B vendors etc.
- **Diversion of products** – These could include high dependence on favored distributors to sell the bulk of stock; kickback received from the distributor/ wholesaler for favorable contractual terms and annuity business; diversion of domestic sales to export market through unauthorized exporters; using substandard parts of substitutes etc.
- **Distribution Management** – These could include failure to report damaged/expired inventory; manual invoicing outside the distribution management system; unauthorized sale of free products/gifts; dummy customers created to inflate sales etc.
- **Transportation fraud** – These could include allocation of business on non-contracted/ non-agreed routes to favored vendors for kickbacks; significant difference in rates at which trucks are hired from the spot market; weighbridge-related fraud, including manipulation of gross/net reported weight of trucks or partial unloading of trucks/ tankers; siphoning off and diversion of goods by transporters

Q 8. What will be the mechanism for training employees, to help curb fraud?

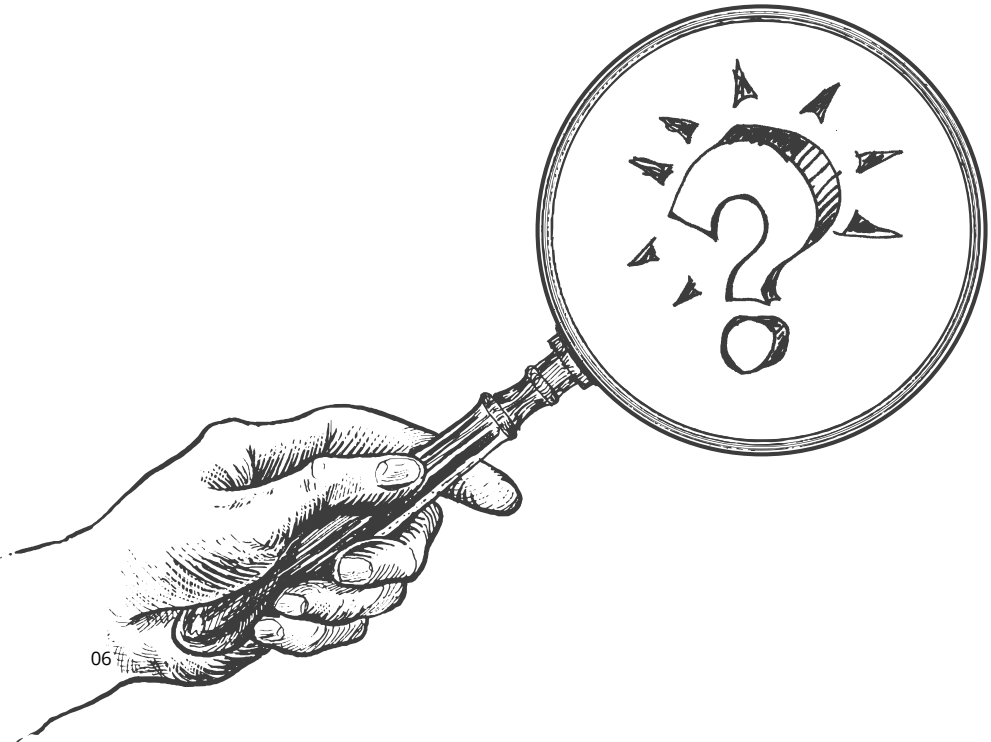
Conducting trainings can help employees understand the companies' policies and procedures as well as help organizations comply with regulatory requirements. Trainings have also shown to have a direct impact on the ability to detect and respond to fraud early, consequently losing much less (financially) to fraud. According to the Association of Certified Fraud Examiners (ACFE) Report to the Nations on Occupational Fraud and Abuse, 2016, companies with anti-fraud training programs were able to detect fraud 40% sooner and lost 50% less to fraud than companies that didn't focus on training.

The mechanism through which these can be carried out are either through face to face traditional classroom sessions for smaller targeted groups of employees or by investing in web based e-learning solutions for larger groups of employees.

Q 9. What action(s) can be taken to curb fraud at big corporates?

Survey findings from Deloitte's India Fraud Survey, Edition II have revealed that fraud risk management efforts need to evolve within large organizations and extend towards understanding/ dealing with emerging frauds. In line with that, we recommend the following measures:

- Have a team in place that focuses on researching new frauds to understand potential emerging fraud risks that may impact your business.
- Organizations must also ensure that fraud risk management controls are periodically updated in line with the business landscape and knowledge of potential frauds, failing which they may not be able to prevent new frauds.
- Automation is the future of fraud risk management. As new data gets generated within organizations, an automated system of continuous monitoring is the way forward and may give successful outcomes provided it is backed by updated policies, controls and rules engines.
- Invest in dedicated employee training programs to help curb fraud. One employee empowered, is one employee less vulnerable to fraud.



Q 10. How do small and medium enterprises address fraud risk as in most cases it is difficult for them to invest in the processes, time and infrastructure (tools) to mitigate such a risk considering other priorities?

One of the common perceptions that small businesses tend to carry is that fraud risk management is a costly, time consuming activity, and hence best approached when the business reaches a certain critical size. However, in our experience, small businesses tend to lose more to fraud - monetarily (as a proportion of business revenues) as well as reputation wise than large businesses. This makes it imperative for them to focus on building effective internal controls.

Small organizations can consider instituting the following measures as a start to their fraud risk management journey.

- **Enhancing the scope of internal audit** – Internal audits can help review accounting processes to validate financial information, discover any errors, test internal controls, and identify any gaps and limit the legal and tax related damages that the business may otherwise suffer.
- **Management certification of financial statements** – This indicates that the business understands the observations made by the audit team (internal and external) pertaining to the organization's financial position, fraud risks, and any other concerns. It also signals a willingness on the part of the organization to address any concerns in the future.
- **Division of responsibilities** – There should not be abundant concentration of job responsibilities in key functions. For example, in the Purchase department, the requestor, negotiator, and approver should be different people. Also, there should be multiple signatories to authorize transactions above a certain threshold. In our experience, some of the functions susceptible to fraud include sales, procurement, cash and bank operations, and employee reimbursement claims process. This can be a starting point for small and medium businesses to initiate division of responsibilities.
- **Undertaking formal fraud risk assessment of key processes** – Whether conducted by third party organizations or undertaken internally, fraud risk assessments of key processes and functions within an organization can help understand the level of fraud vulnerabilities better. If it is conducted internally, it should be conducted by personnel having in-depth knowledge of the business and market with knowledge and experience of fraud. Some of the suggested processes that should be regularly reviewed include Sale (order to cash) process, Procurement (procure to pay) process, Inventory management, Financial reporting and closing (record to report) process, cash and bank operations, and employee expense reimbursement claims process.
- **Defining a code of conduct** – A code of conduct which is tailored to the needs of the organization and adequately covers anti-fraud clauses, can help set the tone among employees/third parties of ethical and unethical practices and penalties associated with undesirable behavior.
- **A channel for employees/third parties to report suspicions** - While most small businesses tend to expect employees to report suspicious activity to their managers, it is also important to provide an independent channel – such as an unmanned complaint box, dedicated email ID, or installing a toll free number, that employees/ third parties may use to report such instances, without fearing retaliation.

Q 11. How is an issue such as a social media smear campaign related to fraud?

A smear campaign is a deliberate attempt to malign an organization (or individual's) reputation, often by revealing selective information or by making up information. There have been instances where parties running smear campaigns have accused the victims of fraud, misconduct or non-compliance. In many cases, the perpetrators tend to lead victims to either download malware or deposit money in return for information. For example, "Company XYZ accused of financial misreporting. Click here to read the full report."

Unfortunately, the onus of tackling these accusations tends to fall on the victim. In the context of social media, it is easy to start a smear campaign against any individual or entity while the perpetrators hide behind the anonymity provided by this platform, making legal recourse a challenge.

Q 12. What is the relation of anti-competition to fraud and misconduct?

Violating the principles outlined in the Competition Act laid down by the Competition Commission of India is a matter of non-compliance and misconduct that can lead to the levy of high penalties/ fines. This can expose organizations to a relatively newer risk in the Indian context–that of their growth strategies and consequent business actions being scrutinized for inappropriate behaviour in regards to competition.

The Competition Act redefines business conduct and some of the traditional ways of doing business may now be looked upon as unacceptable business practices. To avoid punitive action under the Competition Act, Indian business organizations need to evolve a strong culture of compliance covering increasing awareness about the requirements of law, robust code of conduct, promoting fair business practices as also individual conduct while interacting with competitors.

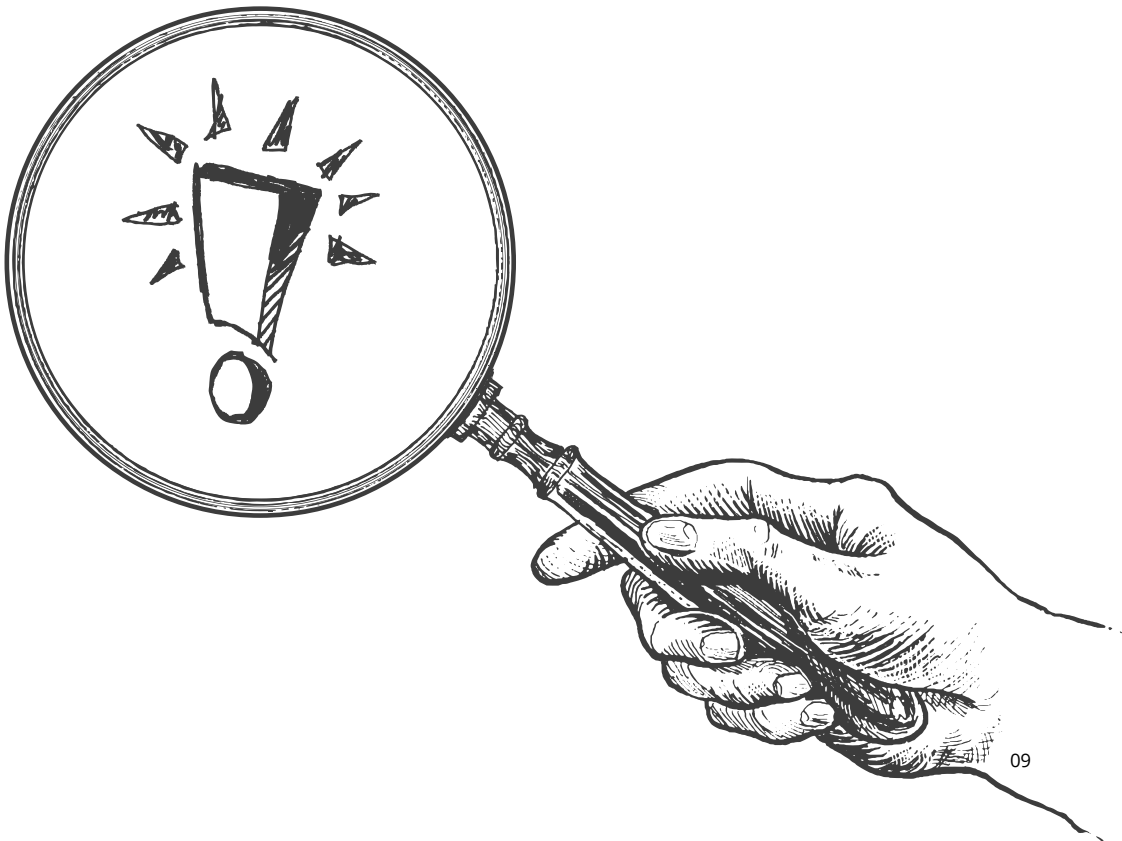
Q 13. What are some of the sector specific trends observed pertaining to fraud in 2017?

- **Frauds specific to the Insurance sector**
  The insurance sector has its share of frauds in the form of claims/ surrender fraud, mis-selling, KYC (Know your Customer)/AML (Anti-money laundering) breaches, commission rebating, forged documentation, employee misdemeanors and collusion between different parties, dealing room frauds (that can manifest itself in different forms like front running, insider trading, price manipulation and other forms of market abuse), data theft; to name a few.
- **Frauds specific to the IT/ ITeS sector**
  Some of the areas most vulnerable to fraud are recruitment, data theft and procurement. Recruitment frauds can take many forms - existence of ghost employees in the company records, collusion with recruitment consultants to recruit otherwise unsuitable candidates in exchange for kickbacks, recruiting employees with fake credentials, unauthorized representation of the organization in colleges, and issuing of fake job offers.
- **Digital frauds particular to the Banking sector**
  The advancement of technology in providing innovative services, combined with the explosive growth in internet banking, has permanently altered the business landscape and how banks manage the risk of fraud. Some of the relevant fraud risks in this sector are Internet Banking/ ATM Fraud (Skimming, Ram Raid etc.), Phishing/ Vishing, Misuse of credit and debit cards and Identity fraud. Further details are available in our survey report titled 'India Banking Fraud Survey, Edition II'

Q 14. How do you tackle fraud caused due to diminishing ethical values?

Diminishing ethical values has been identified as one of the key reasons for fraud (substantiated in Deloitte's India Fraud Survey, Edition II as well). In order to tackle this, a strong ethical culture and social control environment needs to be established within an organization. Some of the following measures can, over time, help develop an ethical enterprise:

- **Code of conduct** – Establish a code of conduct that is periodically reviewed, and acknowledged/accepted by employees and third parties. The policy should include specific clauses pertaining to fraud; that is revised periodically basis the changing fraud risk landscape.
- **Align rewards system with core values** - Include ethical behavior as a key component of employee performance appraisal. Recognize, celebrate and incentivize (if necessary) ethical behavior.
- **Undertake ethical internal reviews to monitor compliance with the code of conduct** – It is necessary to constantly evaluate trends in the volume or nature of unethical behavior reported. This will help determine if steps need to be taken to improve actions regarding the ethics program. Senior management can look at performing periodic ethics assessments, including third party ethics internal reviews.
- **Training/awareness programs, workshops and surveys** - Conduct fraud and ethics survey to understand disconnects between the leadership's 'tone at the top' versus the activities at the ground level. Build awareness with regard to issues such as fraud trends, damage due to fraud including practical scenarios that fraud can manifest itself in. It is also helpful to conduct ethical dilemma workshops for employees for identifying emerging issues.
- **Establish a whistle blowing system** – It is important to provide a channel for your employees and third parties where they are encouraged to report unethical behavior, fraud or misconduct. Proper records of all disclosures should be maintained and the system should be evaluated periodically for its effectiveness.
- **Tone at the top** - The senior management needs to demonstrate zero tolerance to fraud, misconduct and noncompliance, whether it is responding to whistleblower complaints or discussing fraud uncovered in the organization.



Q 15. How do you control sharing of confidential information with competitors?

Sharing confidential information outside of your organization, is usually a breach of conduct and may be construed as an act of fraud. However, in our experience, exiting employees tend to carry confidential information with them. The easy availability of large capacity portable storage devices, cloud-based storage solutions, smartphones and tablets has made it easier for exiting employees to store (and possibly steal) companies' sensitive information. However, organizations can safeguard themselves from such data theft by considering the following aspects:

- Have a comprehensive record of the data held by the organization - Sensitive information tends to be dispersed among departments or business units. To prevent any data theft, it's important for companies to have a comprehensive record of the data they hold.
- Understand the access provided to every employee on company data. This access should be revoked when an employee leaves the company.
- Undertake 'exit checks' on devices owned by exiting employees to understand whether confidential data has been copied to a USB device, uploaded to a personal cloud based account or deleted from the company's IT network. Further analysis on the kind of data accessed by the employee can also help understand the employee's future use of the data. For instance, a manager level resource storing the resumes of junior level resources on a USB drive can be construed as a possible indicator of his/ her attempt to poach these employees in the future.
- Establish a framework for Network Access governance in place. Large organizations often provide varying degrees of access to employees on the data residing in their systems. Only select employees have access to confidential information, others receive such access on a need basis.

For any further queries, please reach out to

Rohit Mahajan
APAC Leader
Partner and Head - Forensic
Financial Advisory, Deloitte India
T: +91 22 6185 5180
E: mahajan@deloitte.com

Amit Bansal
Partner
Forensic – Financial Advisory
Deloitte India
T: +91 22 6185 6764
E: amitbansal@deloitte.com

Jayant Saran
Partner
Forensic – Financial Advisory
Deloitte India
T: +91 124 679 3607
E: jsaran@deloitte.com

KV Karthik
Partner
Forensic – Financial Advisory
Deloitte India
T: +91 22 6185 5212
E: kvkarthik@deloitte.com

Nikhil Bedi
Partner
Forensic – Financial Advisory
Deloitte India
T: +91 22 6185 5130
E: nikhilbedi@deloitte.com

Rajat Vig
Partner
Forensic – Financial Advisory
Deloitte India
T: +91 124 679 2905
E: rajatvig@deloitte.com

Sumit Makhija
Partner
Forensic – Financial Advisory
Deloitte India
T: +91 124 679 2016
E: sumitmakhija@deloitte.com

Deloitte.