Deloitte.

India Corporate Fraud Perception Survey 2018

Edition III

For Private circulation only

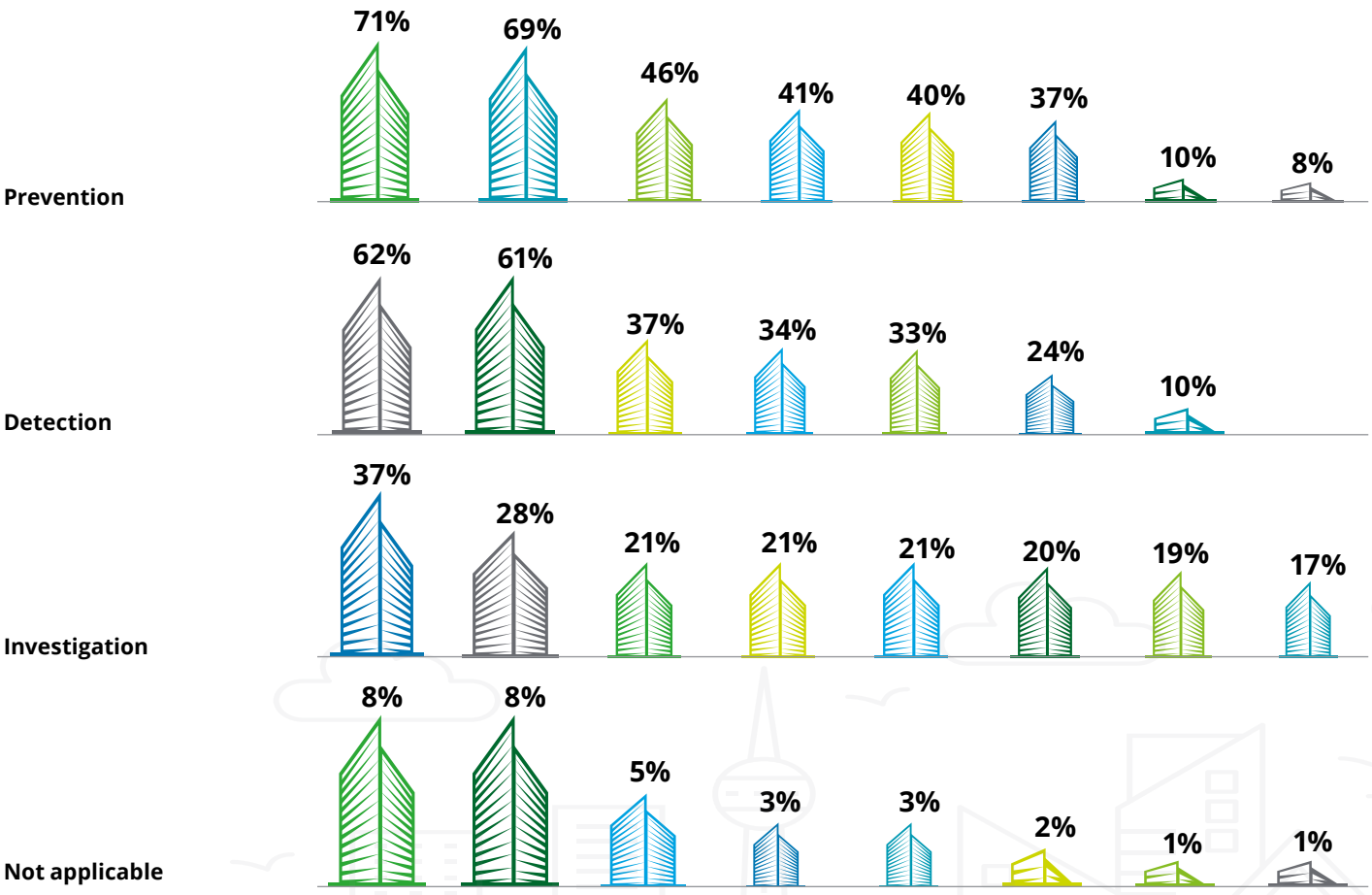
Forensic

Section 2

The approach to fraud prevention, detection, and response

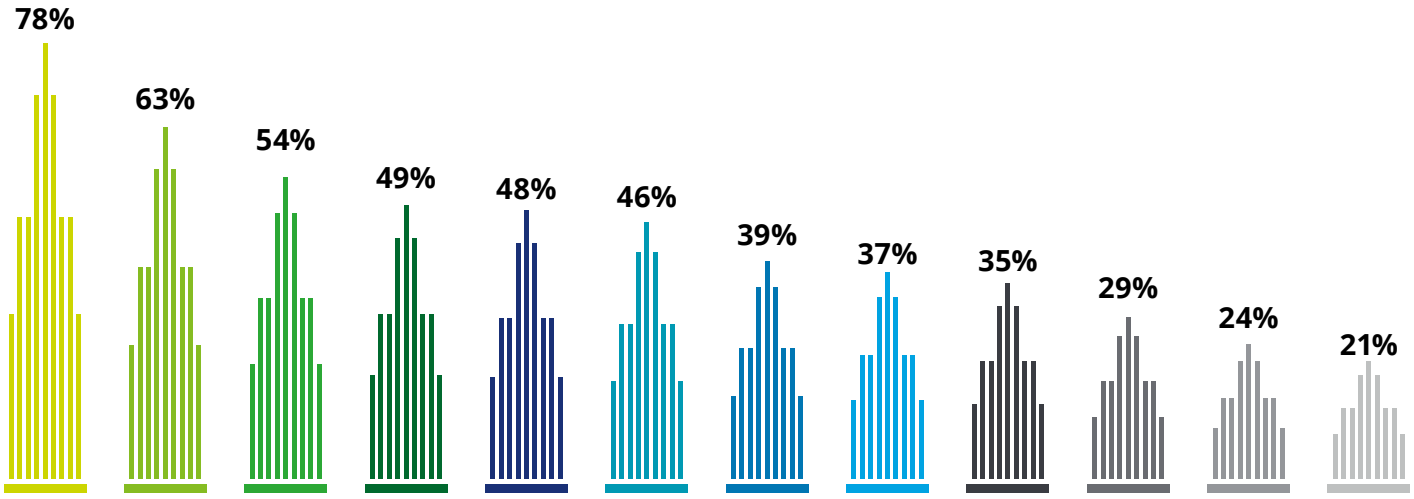
Key Findings

Accountability for fraud: The majority of respondents said that the Board and CEO/ Managing Director had a responsibility to prevent fraud, whereas fraud detection was the responsibility of internal and external auditors. Fraud investigation was identified as the responsibility of the audit committee and the board.



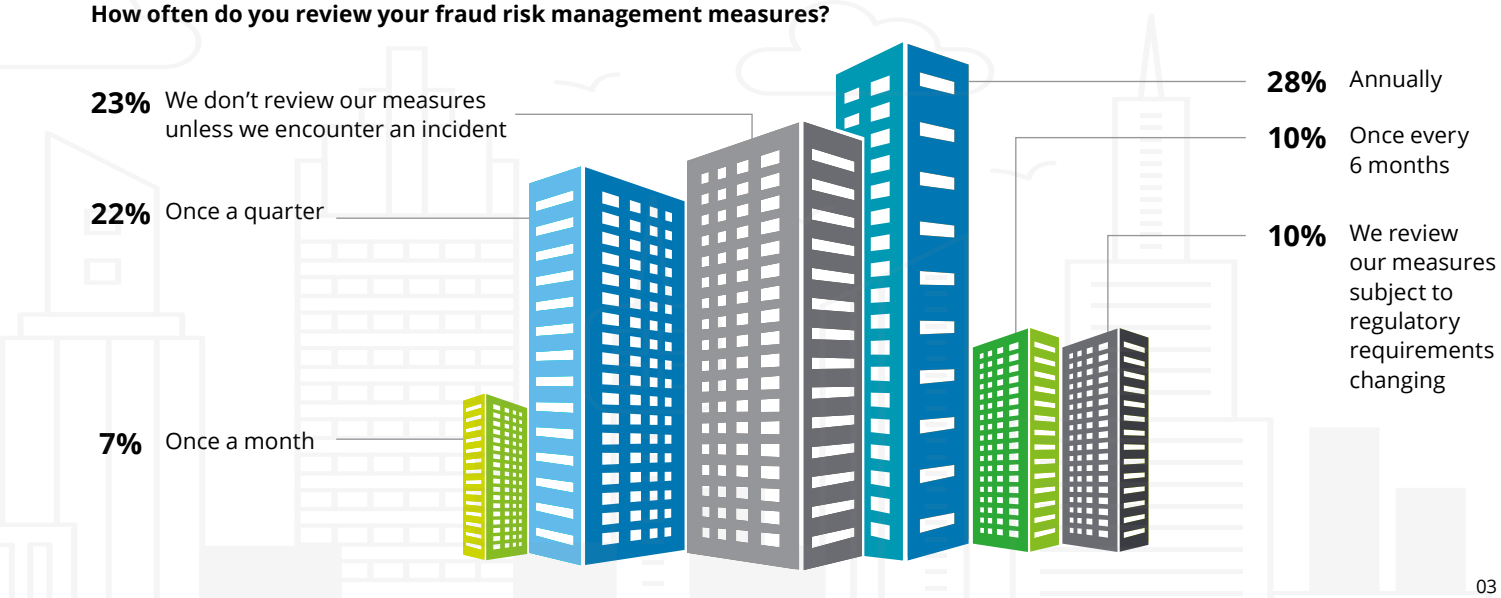
The top three measures taken to prevent fraud include: instituting periodic internal audit, taking serious action and using that to set an example within the organisation, and asking independent auditors to conduct audit regularly. Fraud risk management measures were reviewed differently by different organisations, with 22% of respondents indicating they did so quarterly and 28% indicating they did so annually. About 23% of respondents said they didn't review their fraud risk measures unless they encountered an incident.

What measures does your organisation adopt to prevent incidents of fraud?



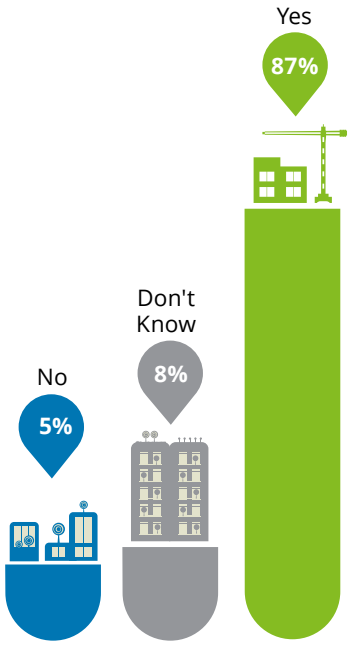
- Institute periodic Internal Audit
- Take serious action in case of incidents of fraud and use such instances to set an example within the organisation to prevent future frauds
- We have independent auditors who conduct periodic audits
- Effective tone at the top, followed by implementing policies for fraud and consequence management, code of conduct, etc.
- Periodic declarations from employees/management on compliance with laws and regulations
- Conduct general fraud awareness trainings/workshops for all employees
- Periodic communication to employees on fraud and its repercussions
- Conducting an ongoing due diligence check (Third party/Senior Management/Business associate, etc.)
- Fraud risk assessment/monitoring of fraud control frameworks—either manually or using technology such as fraud analytics and fraud management systems
- Dedicated training programs for select teams/individuals to address frauds to which organisations are generally most susceptible, such as bribery and corruption, conflict of interest, procurement fraud, etc.
- Engage third party forensic experts to assess our fraud risk management frameworks at least once a year
- Dedicated fraud prevention unit that researches new frauds and communicates them to the fraud risk management teams

How often do you review your fraud risk management measures?

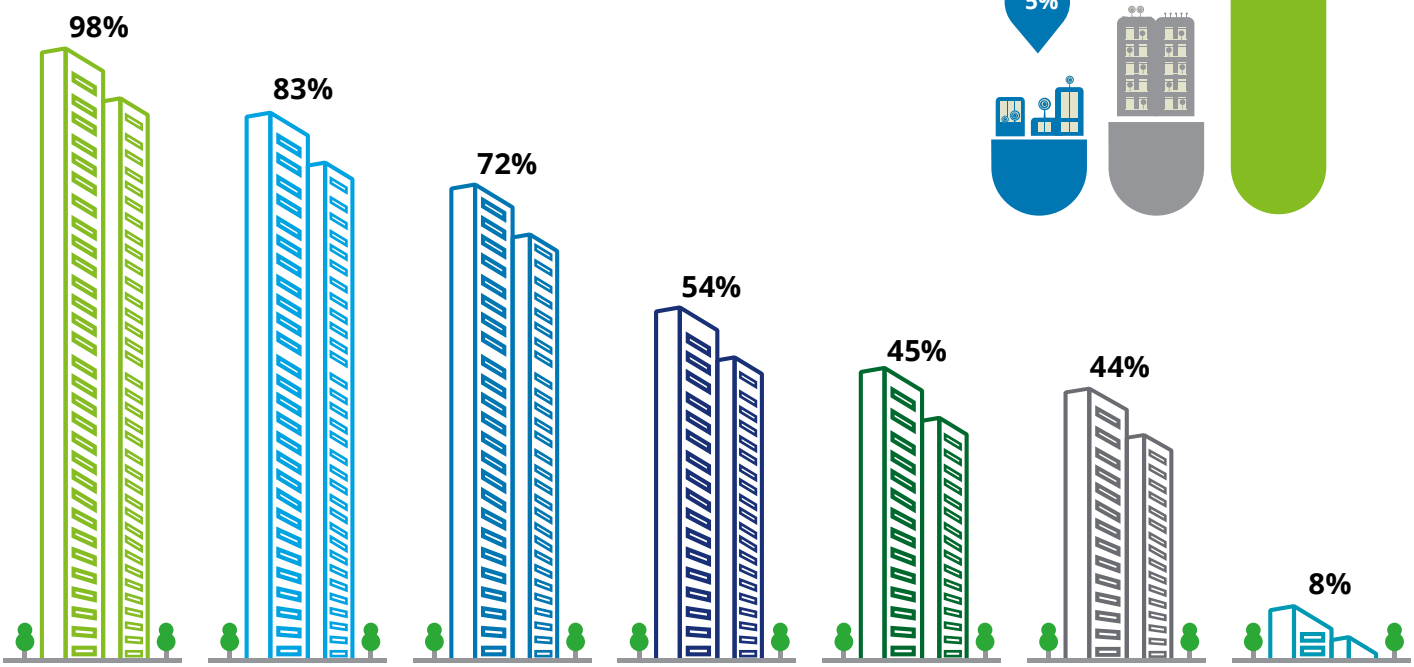


A majority of respondents (87%) said fostering an ethical mindset among employees could prevent fraud in the long term. In line with this, the top three approaches taken to improve the ethical culture within the organisation include: Instituting strong penalties for unethical behaviours, creating a platform to openly discuss ambiguous issues and identify unethical behaviours, and developing training courses and reading material, including case studies, on how ethical behaviours apply in the corporate ecosystem.

Do you believe fostering an ethical mindset among employees can prevent fraud?



Which of the following measures have you considered with an aim to propagate and strengthen the ethical culture within your organisation?



Instituting strong penalties for unethical behaviours

Creating a platform to openly discuss ambiguous issues and identify unethical behaviours

Developing training courses and reading material, including case studies, on how ethical behaviours apply in the corporate ecosystem

Instituting a mechanism to monitor signs of unethical behaviour among employees

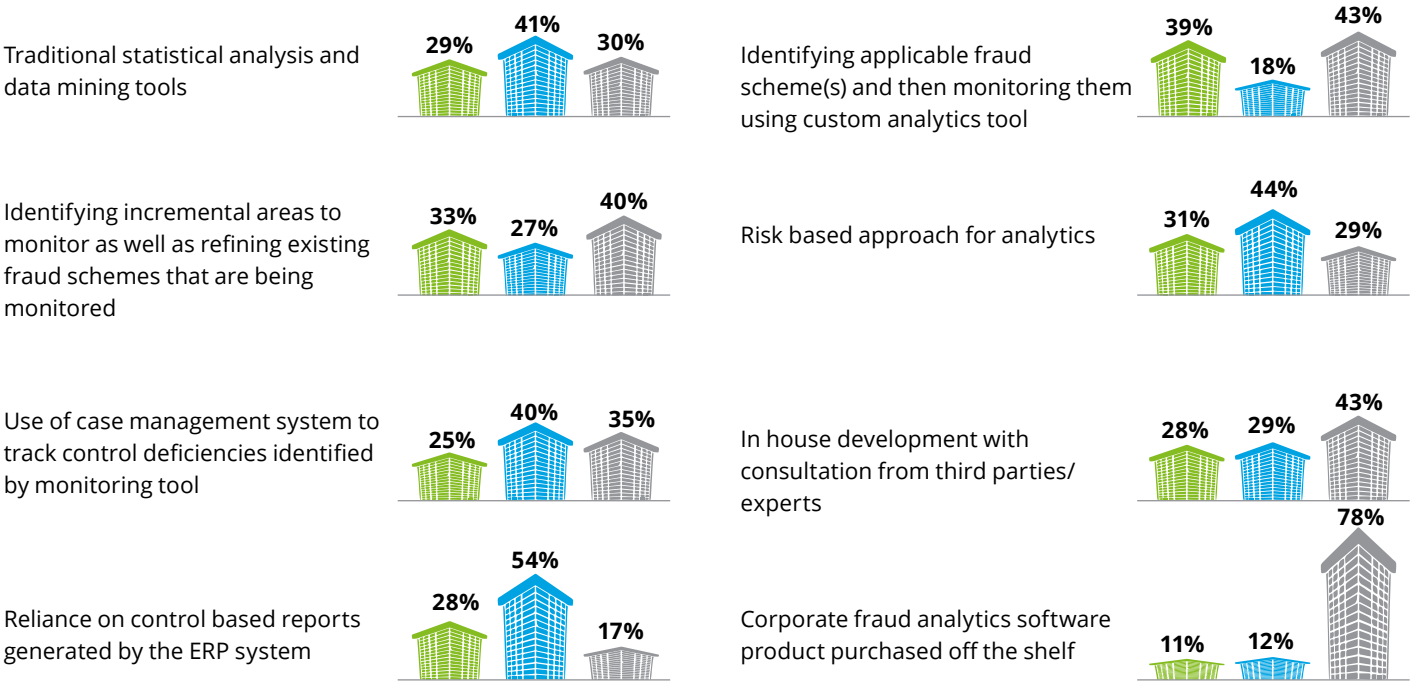
Undertaking an ethics survey to ascertain prevailing employee sentiments towards fraud

Creating rewards and recognitions programs specifically validating ethical behaviours

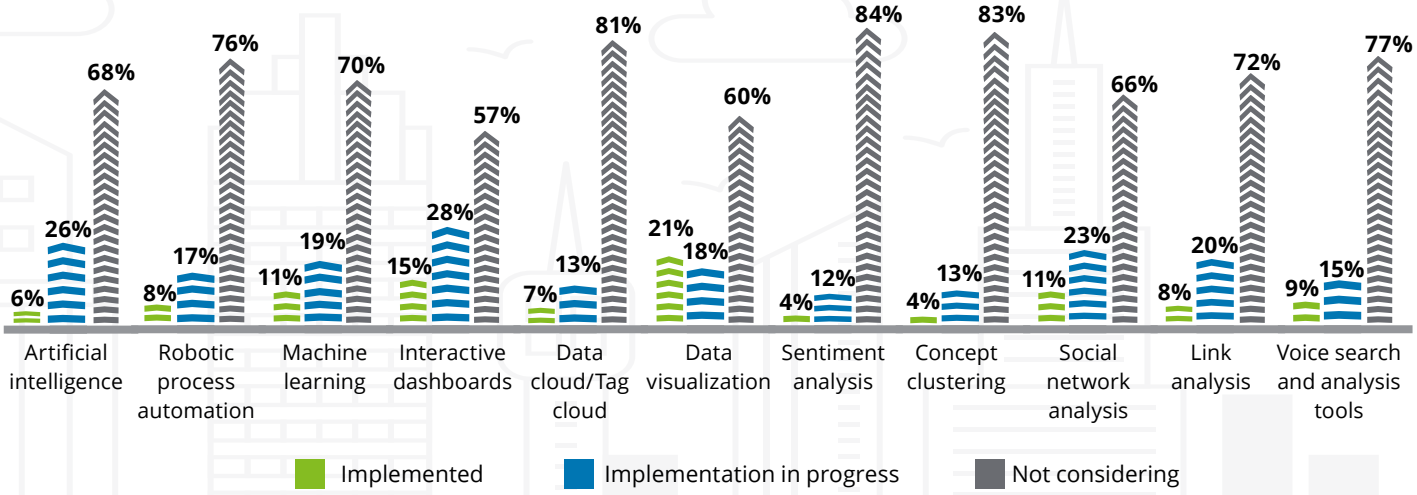
Others

Use of technology to mitigate fraud risks is on the rise with respondents identifying the following most commonly used techniques/ tools to prevent fraud: reliance on control based reports generated by the ERP system (54%), risk based approach for analytics (44%), and traditional statistical analysis and data mining tools (41%).

To help continuously monitor controls, which of the following technologies/applications/approaches have you considered?

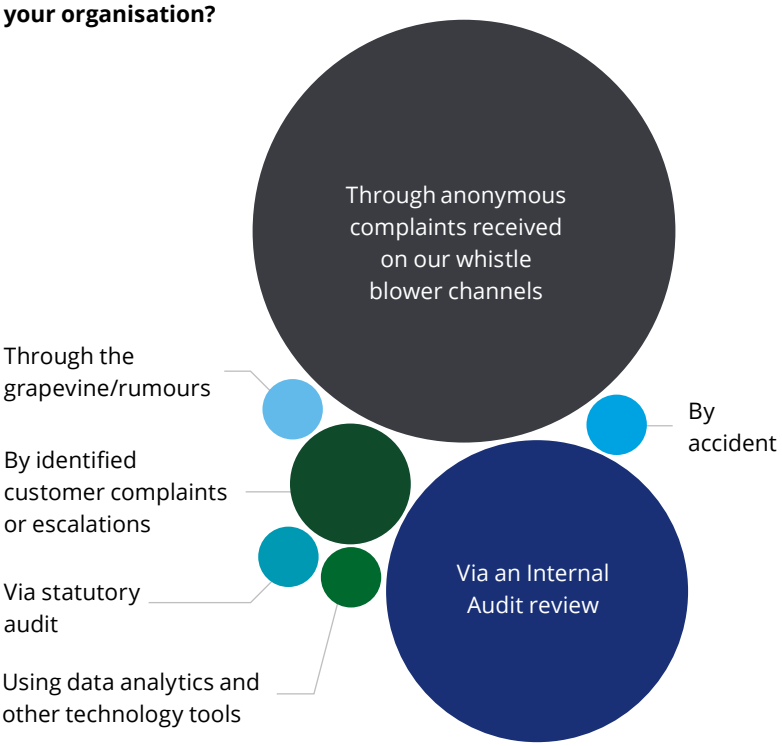


There is increasing awareness of advanced technologies in fraud detection with around a fourth of all respondents saying they had implemented or were implementing tools/ techniques such as voice search and analysis, link analysis, social network analysis, sentiment analysis, data visualisation, interactive dashboards, machine learning, robotic process automation and artificial intelligence.

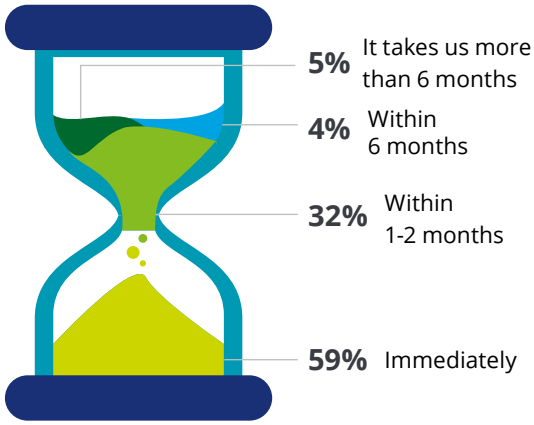


Fraud is detected primarily through whistleblower hotlines, followed by an internal audit review. About 59% of respondents indicated that fraud related observations were addressed immediately, by way of commencing investigations – internally or assisted by third parties. All acts of suspected fraud were treated with the same sense of urgency, irrespective of the potential financial and reputational implications.

How are potential fraud incidents typically detected in your organisation?



How urgently are any high potential fraud related observations addressed?

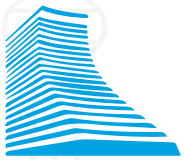


Upon identifying an instance of fraud, which of the following factors is likely to drive a stringent course of action in your organisation?

42%
Any act of fraud is dealt with in the same manner

20%
Materiality– potential value of fraud/loss

16%
Reputational loss caused to the organisation as a result of the act



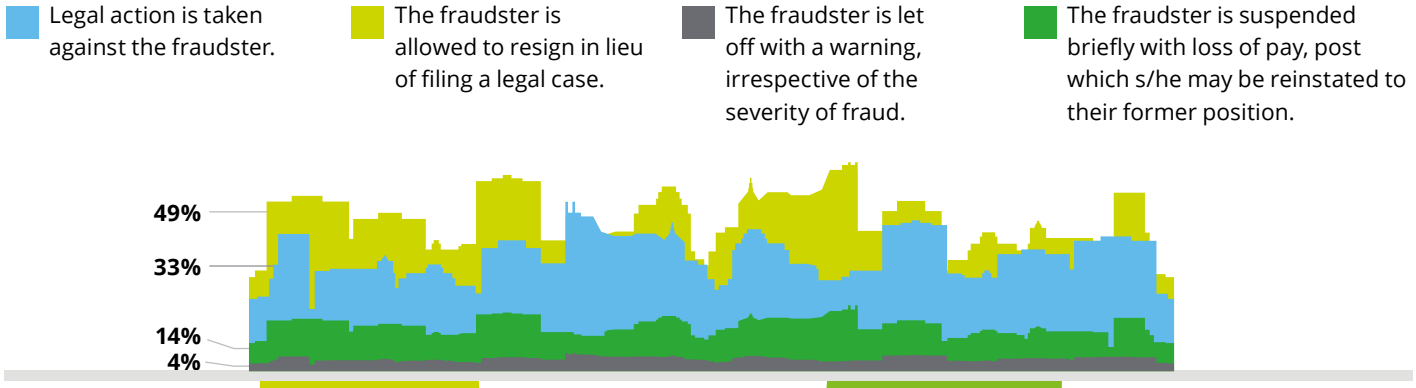
12%
Whether the act has also resulted in regulatory non-compliance

7%
Seniority of perpetrator in the organisation

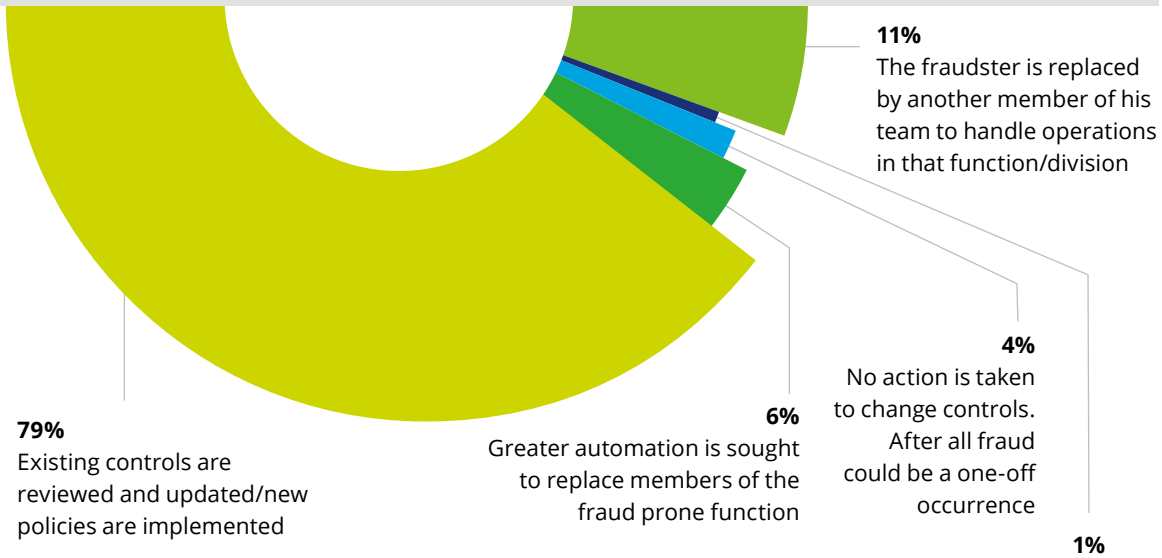
3%
Whether the act has also affected external stakeholders

Once the fraud was ascertained, the fraudster was allowed to resign in lieu of filing a legal case in the majority of cases (49%). However, a third of respondents indicated that they took legal action against the fraudster. Further, existing controls were reviewed and updated/new policies were implemented post the incident, 78% of respondents indicated. The fraud was communicated to the Board and regulatory authorities (where applicable) as indicated by 35% of respondents.

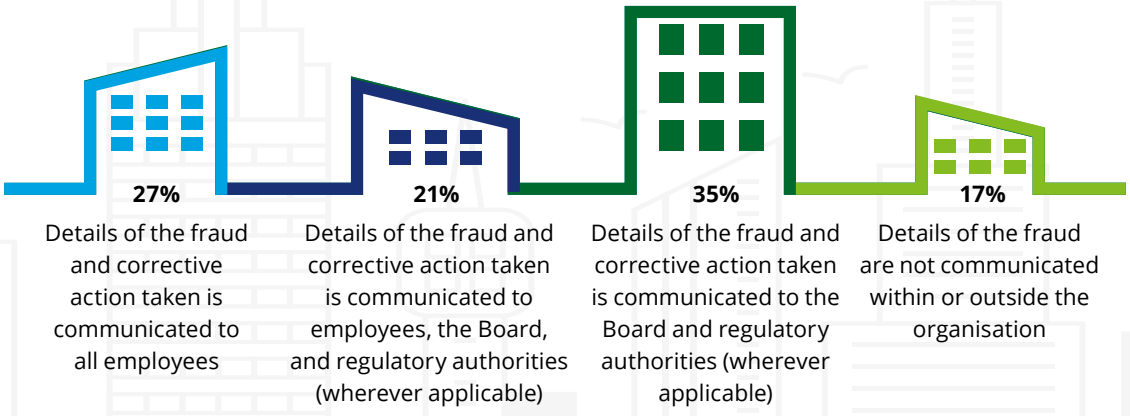
In the area of 'taking action on the fraudster(s) post investigation', my organisation best responds as follows



In the area of 'addressing controls', my organisation best responds as follows



In the area of 'Communication of action taken on fraud', my organisation best responds as follows



Some questions allowed for respondents to provide multiple choices. For those questions, the total percentage will exceed 100%.

Our observations

Technology is helping organisations to proactively manage the risk of fraud. In the last two years, it appears that organisations have implemented several tools to assist them in monitoring transactions and flagging off suspicious entries. We believe these investments in technology have been successful, thereby prompting corporates to look at the next level of technologies for fraud prevention. As the adoption of newer technologies by large organisations commences, we expect some of these tools to become more affordable over time for mid-sized organisations to also adopt. Alongside, this technology adoption, it is essential that investments be made in training of resources to optimally utilise these tools.

In the area of fraud response, there appears to be a change in how the fraudster is dealt with. Bolstered by regulatory reforms, more organisations appear to be seeking legal recourse to fraud. In such a situation, it is essential to understand how to preserve evidence in a legally acceptable manner. In our experience, most internal fraud prevention units and internal audit teams prefer to work with third party experts for this activity as well as for quantification of losses.

There is also recognition among corporates of the fact that a change in culture towards zero tolerance to fraud is essential to prevent future instances of fraud. While institutional measures are necessary to impart education and awareness among employees, it is also essential that line managers create an environment that is conducive for their teams to raise concerns without fearing retaliation or bias. In our experience, open discussions within teams on misconduct and malpractice, alongside managers living and demonstrating ethical behaviors can accelerate the creation of an ethical enterprise.

Key contacts

Nikhil Bedi
Partner and Leader – Forensic
Financial Advisory
Deloitte India
+91 22 6185 5130
nikhilbedi@deloitte.com

Partners within Deloitte Forensic's practice in India

Ajay Singh
ajaysingh@deloitte.com

Amit Bansal
amitbansal@deloitte.com

Arjun Rajagopalan
rarjun@deloitte.com

Jayant Saran
jsaran@deloitte.com

KV Karthik
kvkarthik@deloitte.com

Rajat Vig
rajatvig@deloitte.com

Sumit Makhija
sumitmakhija@deloitte.com

Wilfred Bradford
wbradford@deloitte.com

Directors within Deloitte Forensic's practice in India

Amol Mhapankar
amhapankar@deloitte.com

Himanshu Arora
himanshuarora@deloitte.com

Kavita Nathaniel
knathaniel@deloitte.com

Nishkam Ojha
nojha@deloitte.com

Rajesh Chawla
rajchawla@deloitte.com

Rohit Goel
rogoel@deloitte.com

Rohit Madan
madanr@deloitte.com

Sachin Yadav
sachyadav@deloitte.com

Saurabh Khosla
khoslas@deloitte.com

Vivek Bhamodkar
vbhamodkar@deloitte.com

Deloitte.