Deloitte.

IOD Institute of Directors Building Tomorrow's Boards

Corporate fraud and misconduct: Role of independent directors

October 2021

Contents

Foreword

The extensive and widespread use of technology in business today while enhancing efficiencies has also provided openings for frauds and associated risks. In this environment, it is important that Independent Directors (IDs) be vigilant, prudent, and understand the risks of a virtual work environment. This responsibility is heightened in the post pandemic world and the evolving regulatory framework. Today, IDs must play a significant role in overseeing the fraud detection and prevention mechanisms. IDs therefore, must equip themselves with the knowledge of key risks and effects that such incidents could have on their organisations.

To this effect, **"Corporate fraud and misconduct: Role of Independent Directors"** offers an in-depth insight into the awareness in the Independent Directors' community on fraud, misconduct, and non-compliance, and their fiduciary responsibilities related to these. The insights in this report have been compiled based on a survey initiated by Deloitte in collaboration with the Institute of Directors (IOD) to understand how IDs perceive corporate fraud, their preparedness in addressing it, and the best practices to mitigate associated risks.

The findings and perspectives laid out in this report will help provide a perspective on the role that Independent Directors play today in addressing corporate fraud.

We hope you find this report informative and thought provoking.

Happy reading!

Atul Dhawan
Chairperson
Partner
Deloitte India

Corporate fraud and misconduct: Role of independent directors

Foreword

Deloitte Touche Tohmatsu India LLP, in association with the Institute of Directors (IOD), has carried out a joint survey to understand how Independent Directors (IDs) perceive corporate fraud, their preparedness for addressing it, and adoption of best practices to mitigate corporate fraud and misconduct risks.

The survey questions were designed to elicit the views of executives and IDs for tackling fraud, bribery, and corruption. The survey clearly brings out how the corporates face and fight fraud and corruption in an era of significant technological advance, despite the introduction of significant anti-corruption laws, and continued escalation of unethical conduct.

Over the years, IDs role has been evolving and enhancing, and regulators are placing increasing dependence on their vital role for good governance. IDs are chairing or are members in majority of the board committees, including the 'Internal Audit Committee'.

Covid-19 has significantly disrupted business environment and has led to numerous challenges that have exposed corporates to fraud related vulnerabilities. A remote workforce has proved to be more vulnerable and exposed to cybercrime, including data theft, breach, and intellectual property frauds.

IDs need to:

- Re-evaluate data protection policies - reassess technology and infra-structure solutions from security perspectives and ensure secured and resilient operations
- Regularly monitor fraud and cyber-security threats
- Deploy crisis management response mechanism
- Be vigilant for financial statement fraud schemes
- Board audit committee to have an effective anti-fraud and misconduct detection mechanism

IDs can play a significant role in pushing the agenda for periodical detailed assessment of organisation's risk management system to control cybercrimes, promote fraud risk management framework, knowledge and training, proper reporting protocol of whistle blowers. In safeguarding organisations against fraud, IDs need to act with the highest standards of vigilance and prudence.

Lt. Gen. J. S. Ahluwalia,
PVSM (Retd.)
President
Institute of Directors

Introduction

Independent Directors (IDs) are key in the overall governance of the organisation and are becoming vital in organisation's efforts to mitigate fraud and associated risks. Over the years, occurrences of large-scale corporate frauds in India has heightened the need to overhaul and strengthen the corporate governance framework to make India more competitive in the globalized world. This resulted in a series of legislation being enacted which enhanced regulatory requirements in dealing with and reporting on corporate fraud . The Companies Act, 2013, and the revised corporate governance norms of the Securities Exchange Board of India (SEBI) for listed companies, have placed significant accountability for fraud risk management on the Board of Directors and audit committee (including IDs).

The growing focus on ethics and corporate governance within organisations has increased the importance of the role of an ID in being an effective deterrent to fraud, mismanagement and lapses in corporate governance.

Further, the business disruption caused by the pandemic has further underscored the need to be vigilant and strengthen governance frameworks as historically, data shows that business disruptions/crises have been followed by not only a rise in new and increased fraud risk vulnerabilities but also by discovery of fraudulent practices committed over the years. The current business environment with its remote working business model, increased technology adoption and with control frameworks not keeping up pace with the change in business models is turning out to be a catalyst for increased fraud risks. In this new scenario of uncertainty induced by Covid-19, it becomes pertinent to raise awareness on fraud, misconduct and noncompliance amongst the ID community, for them to effectively discharge their duties.

Against this background, Deloitte Touche Tohmatsu India LLP (DTTILP) in association with the Institute of Directors (IOD), has carried out a survey to understand how IDs perceive corporate fraud, their preparedness in addressing corporate fraud, and the adoption of best practices to mitigate fraud and misconduct risks.

The survey observations reflect an expected rise in frauds in near future and a need for IDs to enhance their awareness of fraud risks/FRM framework to enable them to be better equipped and discharge their duties. Accordingly, IDs should reflect on the changing fraud risk landscape faced by organisations in the evolving complex business environment and carefully evaluate the effectiveness of the organisation's fraud risk management strategy.

Although there are multiple priorities for those charged with corporate governance, in our view, there is a need for IDs to reflect upon the level of their organisations preparedness to meet the challenges of fraud and misconduct in the current environment and accordingly should empower themselves to preserve organisation value and fulfill their fiduciary responsibility.

Nikhil Bedi
Partner and Leader – Forensic,
Financial Advisory
Deloitte Touche Tohmatsu India LLP

[1] Companies Act, 2013; SEBI Guidelines – LODR, Constitution of National Financial Reporting Authority, SEBI guidelines for disclosure of any forensic audit,and the standards for forensic accounting and investigations in India issued by ICAI.

Executive Summary

Around **63 percent** of the IDs responded that the current business environment induced by the pandemic can spur fraud over the next two years. Large-scale remote working **(21.79 percent)** and cash flow crunch leading to business operations taking a priority over compliance **(20.09 percent),** were identified as the key factors for the expected rise in frauds.

Cybercrimes **(23.90 percent),** financial statement frauds **(20.96 percent)** and leakage of sensitive information including insider trading **(12.87 percent)** are most likely frauds to be experienced in the near future.

Around **58 percent** IDs believe that organisations should focus on fraud prevention and prediction techniques to improve their FRM framework and minimise fraud risk.

Approximately **75 percent** IDs believe that they could play a significant role in preventing, detecting and responding to fraud, however, close to **54 percent** expressed a need to be better equipped to discharge their fiduciary responsibilities.

While around **57 percent** IDs indicated that their board had established an effective FRM framework, around **22 percent** IDs indicated the need to increase awareness amongst employees on ethics, integrity, and reporting fraud or misconduct issues to improve the FRM framework.

After receiving suspicious activity reports, around **63 percent** IDs responded that they would suggest a preliminary analysis to ascertain the veracity of the allegation and may consider appointment of an independent expert to conduct an investigation.

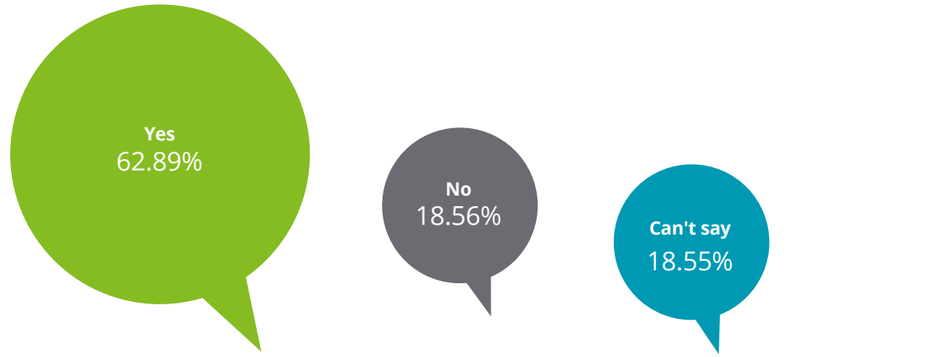
Section 1

From the watchtower: The future of fraud

Key findings

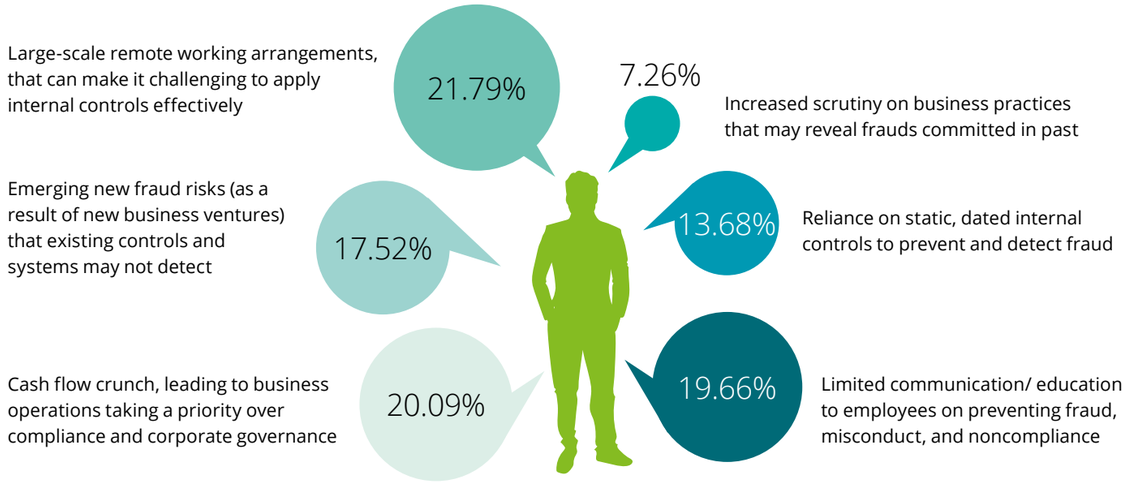
– Around 63 percent IDs feel that the current business disruption can spur fraud over the next two

Do you believe that the current business disruption can spur fraud over the next two years?
(Please select one option)



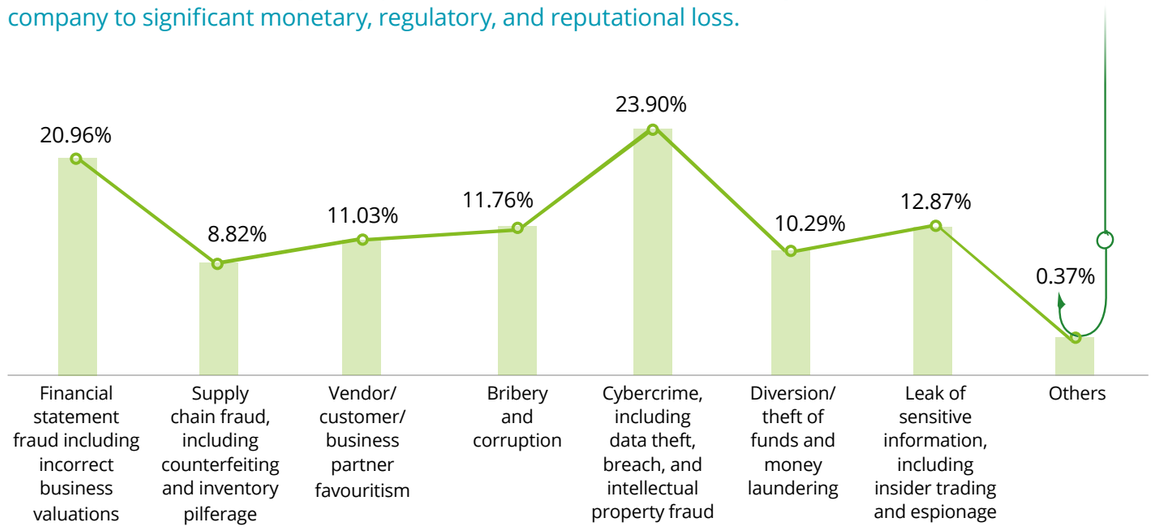
– Large-scale remote working arrangements (21.79 percent), cash flow crunch, leading to business operations taking a priority over compliance and corporate governance (20.09 percent), and limited communication/ education to employees on preventing fraud, misconduct, and noncompliance (19.66 percent) are the key factors for the expected rise in the future fraud.

What do you feel are some of the factors/ pressures that can contribute to frauds in the future?



– Cybercrimes (23.90 percent), financial statement fraud including incorrect business valuations (20.96 percent) and leakage of sensitive information, including insider trading and espionage (12.87 percent), are the most likely fraud schemes to be experienced in the near future.

From the list below, identify the top three frauds and malpractices that you believe can expose the company to significant monetary, regulatory, and reputational loss.



Observations

COVID-19 has significantly disrupted business environments and has led to numerous changes such as, change in business models, cash flow crunch, and remote working environment, which have exposed organisation/individuals to increased fraud-related vulnerabilities. This is in line with the survey responses, where around 63 percent IDs responded that they believe fraud will increase over the next two years.

While there are multiple aspects that add complexity to the overall environment, certain elements are more important than others, for instance:

- The sudden shift to remote working resulted in multifold increase in electronic communications, both written and verbal wherein employees were working in a less-secure environment. New workflows to accommodate processes, coupled with limited oversight, may have created opportunities for both internal and external parties to commit fraud.

  In-line with this trend, large-scale remote working environment (21.79 percent) was identified as one of the key factors that can contribute to frauds in the near future. A remote workforce has also proved to be more vulnerable to cyber-attacks, such as phishing attempts or "whaling" scams that trick recipients into downloading malware or unknowingly providing confidential and sensitive information. These changes in business operations have exposed organisations to heightened risk of cybercrime, including data theft, breach, and intellectual property fraud as indicated by 23.90 percent of IDs and leakage of sensitive information, including insider trading and espionage, as indicated by around 12 percent of IDs. Further, the Indian Computer Emergency Response Team (CERT-In) recorded over 6.07 lakh cyber security incidents in the first six months of 2021,[2] which is a significant increase over previous years.

- On the other hand, increased volatility in the businesses as they struggle for survival acted as a rationalizing factor for organisation's management/employees committing fraud. Such acts may have been justified as "tiding over the crisis" to meet stakeholder expectations. Historical data also indicates that the recession that began in 2008, resulted in a significant increase in lawsuits based on fraudulent loss. The President and CEO of the Association of Certified Fraud Examiners quoted, *"With the current historic drops in markets around the world due to the coronavirus pandemic, many of the factors that were present then in 2008 are likely to apply today. During the recession, we can expect not only more fraud to occur, but also more existing fraud to be discovered. It's not a question of if we see more fraud, it's a question now of how much we will see".* Further, as witnessed during financial crises in the past, frauds may have been concealed for an extended period of time, are more prone to be revealed/unearthed amidst downturns when fraudsters can no longer cover up instances of wrongdoing.

  A similar sentiment also emerged from the survey findings, wherein around 21 percent IDs expect a rise in financial statement fraud, including the risk of misrepresenting business valuations which may expose the organisations to significant monetary, regulatory, and reputational loss in the near future.

- Inadequate/redundant controls in a changed environment resulting in newer fraud risks and limited communication/ education to employees on preventing fraud, misconduct, and non-compliance creates a significant vacuum for fraudsters to take advantage of. Approximately 20 percent IDs felt that lack of awareness amongst employees on preventing fraud, misconduct, and noncompliance will contribute to the increase in frauds in the near future. Coupled with the fact that business priorities may take precedence over compliance in time of crisis, there could be situations that some organisations may not have fraud prevention as a priority area, which may contribute to an increase in frauds.

[2] More than 6.07 lakh cyber security incidents observed till June 2021: Government - The Hindu

Addressing heightened cybercrime and financial statement fraud risks: Our perspective

The pandemic has enabled organisations to change the way they operate and redesign their operating model. With this, organisations need to be agile and refresh their fraud prevention plans to align with the new normal. In this context, IDs can play a significant role in pushing the agenda in board meetings, to control cybercrime and keep an eye out for possible fraud incidents.

Drive the agenda to control and monitor cybercrimes

Organisations can achieve a resilient remote working culture by enabling the following actions:

- Re-evaluate data protection policies and controls to secure the ecosystem
- Re-assess technology and infrastructure solutions from a security, capacity, availability, and resilience perspective
- Implement solutions that help monitor frauds/cyber security threats and log events to ensure secure and resilient operations
- Plan, analyse, prepare, and deploy crisis management response mechanisms to mitigate the impact of any business continuity threat
- Re-evaluate the risks arising from third-party ecosystems in the remote working scenario for all employees
- Establish comprehensive policies and procedures to define guidelines for effective working and governance, adapted to the new normal
- Ensure that company conducts periodic awareness drive to sensitise the employees on the risks and precautions to be taken
- Continuously measure crisis response effectiveness on an ongoing basis with regular and rigorous training, testing, and communication

Tips to watch out for cybercrime incidences:

- Understand trends of cyberattacks/ breaches/ attempts in industry and implication thereof on the company's risk profile
- Ensure periodic review of the critical organisational data which is vulnerable to such attacks
- Identify instances of lack of right-fit of technologies and skilled resources in view of the emerging trends
- Understand the fraud trends emerging from third-party eco-systems

Drive the agenda over financial reporting process

While the primary responsibility of financial statement preparation and reporting remains with the management of the organisations, IDs need to be vigilant for control over financial reporting and fraud schemes. Some best practices include:

- Ensuring that the organisation has a robust system of anti-fraud controls over financial reporting and has implemented a continuous monitoring mechanism to identify red flags on a near real-time basis
- Ensuring that the board gets qualitative information (accurate and comprehensive reports) well in advance to review and obtain confidence on the accuracy, completeness, and quality of the information presented
- Ensuring that all material/extraordinary transactions are brought to the notice of the board and have appropriate business justification substantiated with satisfactory information/documents
- Confirm that the related party transactions/extraordinary items are justified, in the organisation's interest and supported with independent subject matter expert's opinions, wherever required
- Apply heightened skepticism and ask challenging questions and record consent or dissent as appropriate
- Consider all whistle-blower complaints/tips diligently and ensure that they are addressed/investigated adequately

Tips to watch out for financial statement frauds:

- Reported financial numbers not in line with the industry and past performance trend
- Complex disclosure notes in the financial statements
- Frequent or ad-hoc changes to the accounting principles adopted for financial statement preparation
- Frequent auditor qualifications or reservations in the audited financial statements
- High employee retrenchment in the finance department or frequent changes to external auditors
- Lack of/inadequate controls over financial reporting

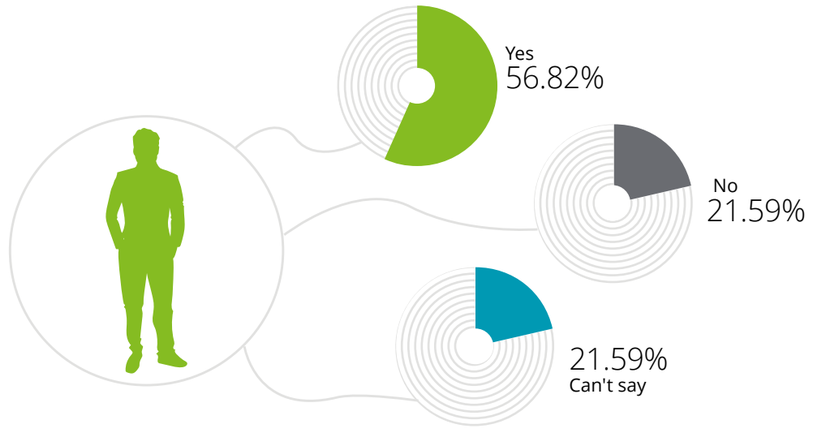
Section 2

Strengthening the foundation – organisation's readiness

Key findings

– Around 57 percent IDs believe that their organisations have an effective anti-fraud and misconduct detection mechanism.

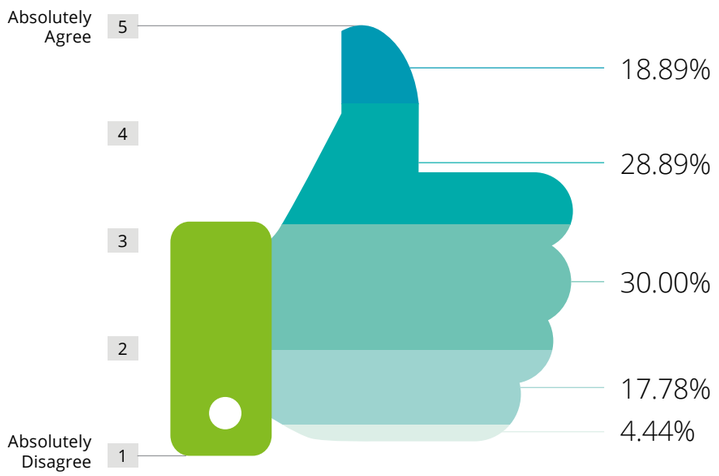
Has the Audit Committee of your board established an effective anti-fraud (including Financial Statement Frauds) and misconduct detection mechanism?



– Around 48 percent IDs responded that the organisations they represent have well-defined and clear incident response protocols to ensure swift actions on detection of fraud and its reporting.

Based on your understanding, please rate the following statement on a scale of 1 to 5, with 1 being "absolutely disagree" to 5 being "absolutely agree".

The organisation/s I represent has well defined and clear incident response protocols to ensure swift actions upon detection of fraud and its reporting



Observations

Fraud risk management is a dynamic phenomenon as the environment, be it internal or external, is constantly evolving. While large organisations have generally set up fraud risk management frameworks relevant in their context, the changed environment has challenged the efficacy of the existing framework, both from a design and implementation perspective. In our view, heightened fraud risks (e.g. cybercrime and fraud due to remote working; logistics and supply-chain fraud, insider trading, and financial statement fraud) and limitations imposed by the disruption (e.g. mobility restrictions, inability to conduct effective due diligence on new third parties, etc.) could have affected the effectiveness of fraud risk management protocols.

Interestingly, we have also witnessed a split response on the existence of effective anti-fraud and misconduct detection frameworks, where on one hand, around 57 percent responded that that the audit committee of the board that they represent have established an effective anti-fraud and misconduct detection mechanism, however approximately 43 percent IDs either did not agree or could not confirm the effectiveness of the existing anti-fraud framework.

As part of a robust FRM framework, it is crucial for organisations to implement a well-defined fraud response plan to minimise damage from the fraud, however, only around 48 percent IDs suggested that the organisations that they represent had a well-defined and clear incident response protocol to ensure swift actions upon detection of fraud and its reporting.

Amidst the rapidly changing environment caused by the pandemic, it is essential for organisations to revisit the effectiveness of existing fraud risk management framework and ensure that the organisations have robust fraud response protocols. A structured approach to calibrate or update the fraud risk management framework will help to steer corporate governance personnel in the right direction, assist them in asking the right questions and ensure the existence of an effective fraud risk management framework both from a design and implementation standpoint.

Organisational vigil in tackling fraud risks: Our perspective

Regulatory requirements in India have recognized fraud as a key risk and have placed responsibility on the board, audit committee and senior management of organisations for development and implementation of a fraud risk management framework. Given the severe economic, reputational, and legal consequences of corporate frauds, organisations today have started taking steps to minimize the fraud risk exposure in their business operations.

While most organisations have developed policies and procedures that cover critical aspects of a comprehensive fraud risk governance framework, several organisations fall short on translating these into practical and functional processes. Given the current disrupted and volatile business environment, relying on traditional anti-fraud mechanisms/controls may not adequately secure the organisation and an updated fraud risk management program – addressing the changing requirements for people, process, and technology - is the need of the hour. Based on our experience, more often than not, the design and implementation of a fraud risk governance framework encounter the following challenges:

- Traditional, case to case-based incidence response approach instead of actively promoting preventive fraud risk control framework and periodic review thereof
- Business priorities takes precedence amidst uncertainties over other matters including compliance
- Lack of a defined structure for the FRM framework and investigation identifying department or person to lead the fraud risk management activities for the organisation
- Set goals and timelines and measure the progress in implementing improvements
- Inadequate awareness efforts to educate employees on their obligations in preventing, detecting and deterring fraud
- Irregular fraud risk assessments of the business processes to determine the fraud risk profile and identify improvement avenues for anti-fraud control framework
- Absence/limited integration of technology in real-time monitoring to identify red-flags and investigative procedures (data analytics tools, computer forensic technologies, etc.)
- Lack of appropriate actions on whistleblower complainants

Section 3

Role of IDs in FRM

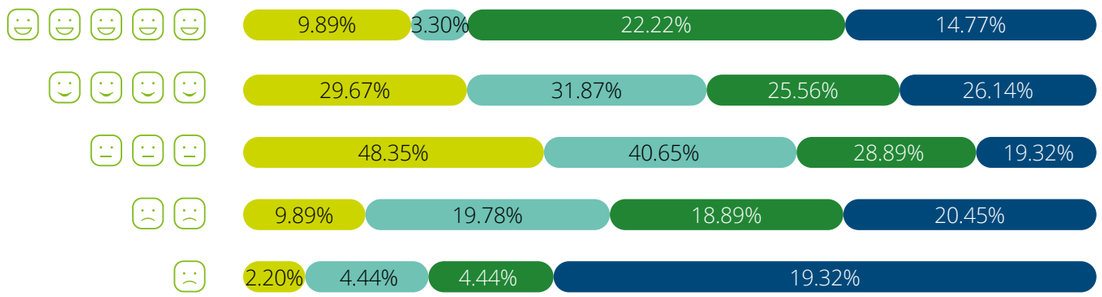
Key findings

– Around 75 percent IDs believe that they could play an important role in fraud prevention and fraud reporting

Do you believe independent directors can play a significant role in preventing, detecting and responding to fraud?

– A majority of IDs indicated a lack of complete understanding of the existing FRM framework and also, did not have comfort on the robustness of the currently implemented FRM framework.

Based on your understanding, please rate the following statements on a scale of 1 to 5, with **1 being "absolutely disagree" to 5 being "absolutely agree".**



- I have been part of atleast three board level discussions involving anti-fraud and misconduct frameworks in the last two years
- The fraud risk management mechanism is reviewed by the board at least once a year
- I believe the current fraud risk management framework (both in design and implementation) is robust enough to mitigate the fraud risks
- I have a complete understanding of the existing fraud risk management structure (both in design and implementation) and how it operates in practice

– Around 76 percent IDs suggest assessments by internal/third-party consultants on the improvement areas suggested by the internal/ statutory auditor to strengthen the fraud risk management framework

What do you typically do upon receiving reports prepared by the internal/statutory auditors of the company, particularly on observations/ improvements in the area of fraud risk management?
(Please select the top three options that applies)

24.00%
Rely on confirmation from the management that the relevant control improvements have been implemented

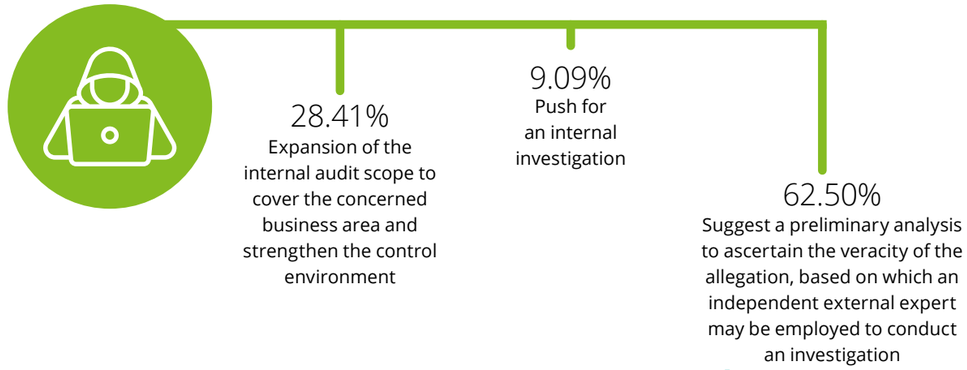
38.00%
Seek an assessment (internal/ third-party) to ascertain fraud risks emanating from the identified controls loopholes as reported in the internal/external audit observations

37.33%
Scrutinize the changes implemented in the controls framework to evaluate appropriateness and effectiveness of the new controls

0.67%
No action is taken

– Around 63 percent IDs indicated that a preliminary analysis should be performed to ascertain the veracity of the allegation, based on which, an independent external expert may be employed to conduct an investigation.

What would you typically suggest upon receiving suspicious activity reports?



28.41%
Expansion of the internal audit scope to cover the concerned business area and strengthen the control environment

9.09%
Push for an internal investigation

62.50%
Suggest a preliminary analysis to ascertain the veracity of the allegation, based on which an independent external expert may be employed to conduct an investigation

Observations

In our view, IDs have a greater responsibility in financial matters, as they make up two-thirds of a board's audit committee under the Listing Obligations and Disclosure Requirements (LODR), including the chairmanship. IDs also oversee the integrity of financial information, risk management, and organisation's vigil mechanism, particularly from a fraud prevention and detection perspective. Per the survey results, approximately 75 percent IDs held similar views as they indicated that they could play an important role, not only in fraud prevention and fraud reporting, but also in helping the organisation respond to fraud instances.

To perform their role effectively, it is important for them to gain a complete understanding of the existing FRM structure (both in design and implementation) and how it operates in practice. Basis the survey responses, it is interesting to note that around 60 percent IDs indicated that they may not have a complete understanding of the existing fraud risk management framework (both in design and practice). In addition, approximately 65 percent IDs believe that the existing fraud risk management framework implemented by the organisations were inadequate to address fraud risks. This could be indicative of the FRM framework not being updated post disruption, reliance on traditional techniques, static data, tick-of-the-box approach, and irregular reviews of the FRM framework by organisations.

On the subject of continuous monitoring, 48 percent IDs have indicated that the FRM is reviewed by the board at least once a year, while approximately 62 percent indicated having been a part of less than three discussions over the last 18 months on FRM practices - indicating a potential lack of periodic review of the FRM frameworks in challenging times posed by the pandemic.

Further, over 63 percent IDs have indicated that in the event of receiving suspicious activity reports, they suggest a preliminary analysis to ascertain the veracity of the allegation. Based on the outcome of such analysis at times an independent external expert is employed to conduct an investigation.

A map for IDs' to build an effective FRM and key challenges ahead: Our perspective

Corporate governance norms have been strengthened by the Companies Act, 2013, and the regulations of the Securities Exchange Board of India (SEBI) for listed companies, where key emphasis is given to frauds by recognising them as a key risk and placing the accountability on the board and senior management. In the case of listed entities, there is an additional responsibility/oversight exercised by "Audit Committee" including IDs on fraud risk management.

Key fraud related by regulatory obligations of IDs
Some key fiduciary responsibilities of IDs include:

01 Obtain comfort on the integrity of financial information, financial controls	02 Ensuring that fraud risk management systems are robust	03 Ensuring that related party transactions are justified and are in the company's interest	04 Seeking appropriate clarification or amplification of information
05 Reporting concerns about unethical behaviour, actual or suspected fraud or violation of the company's code of conduct or ethics policy	06 Ascertaining and ensuring that the company has an adequate and functional vigil mechanism	07 Being cognizant of not disclosing confidential information such as unpublished price-sensitive information and commercial secrets	08 Assessing the quality, quantity, and timeliness of the flow of information between the listed entity's management and the board of directors.

In our view, as the fraud risk landscape evolves, there is a need for IDs to closely and continuously monitor the risks emanating from the changing business environment and periodically drive the agenda on the board to revisit the existing fraud risk management framework.

While the ID community is well versed with their obligations to fulfil their fiduciary responsibilities, at times, the ability of IDs to deliver on these expectations are hampered by limitations or challenges, some of which are highlighted below:

- Due to absence of adequate training and guidance, IDs at times may lack in-depth knowledge of effective FRM programmes
- In certain cases, limited/ infrequent discussions in the board/audit committee meetings about fraud risks that organisations face and improvement requirements of the FRM framework
- At times, lack of timely access to critical information might affect the ID's capability to effectively perform their tasks. In addition, distortion of facts with the volume and complexity of the data involved could also provide additional challenges for IDs to analyze and take the right decisions
- Limited involvement in some cases could impact the ability of IDs to delve deeper into governance and other matters

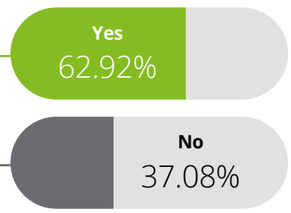
Section 4

Prepping for the future against fraud

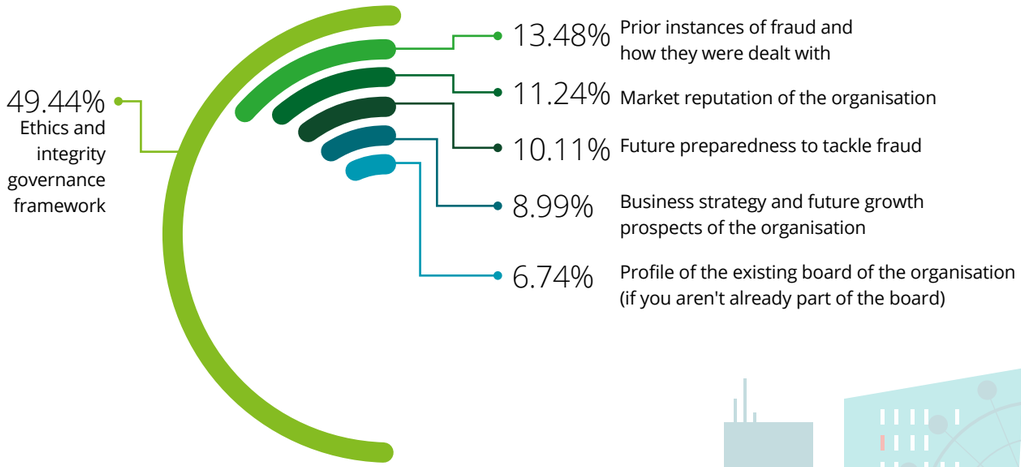
Key findings

– Around 63 percent IDs are agreeable to be a member of the board of directors of an organisation that has previously experienced/reported fraud, however, around 50 percent IDs felt that the maturity of ethics and the integrity governance framework will be a key factor in making this decision.

Would you choose to be a part of a board that has previously reported/ experienced fraud?

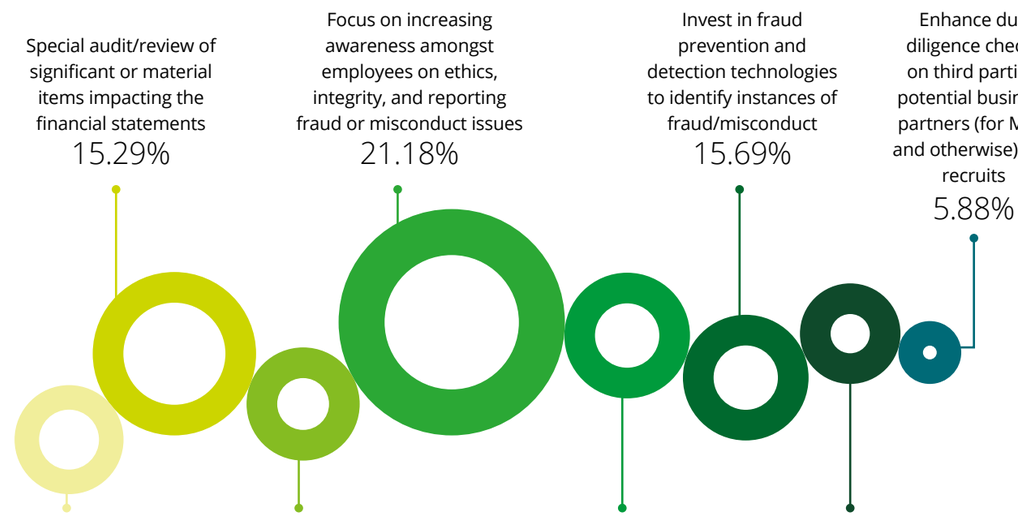


What would be your areas of consideration when making this decision? (select one)



– Focusing on increasing awareness amongst employees on ethics, integrity, and reporting fraud or misconduct issues (21.18 percent), investing in fraud prevention and detection technologies (15.69 percent) and special review of significant material items (15.29 percent) are amongst the best practises suggested by IDs to improve FRM practices.

Given the long-term impact of the current business disruption, what are the best practices that organisations can focus on to improve their fraud risk management practices? (Please select top three)



10.20%
Enhance focus/ scrutiny on the financial reporting process

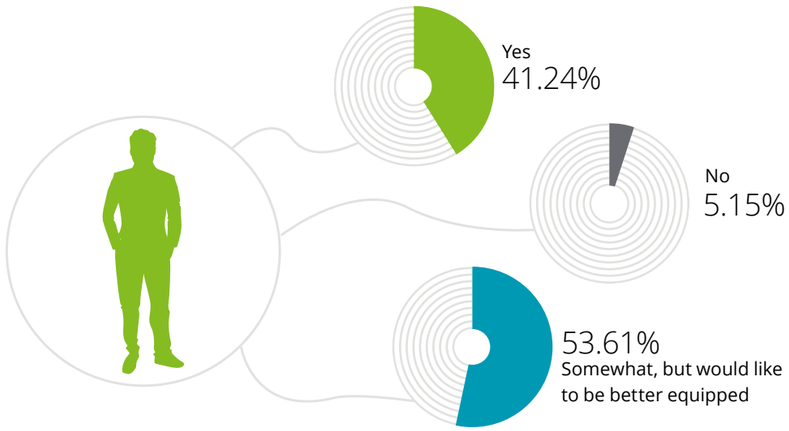
10.59%
Enhance fraud/ misconduct monitoring of business operations

11.76%
Set up an efficient whistle-blower and redressal mechanism

9.41%
Engage independent forensic experts to assess organisational fraud risk management frameworks

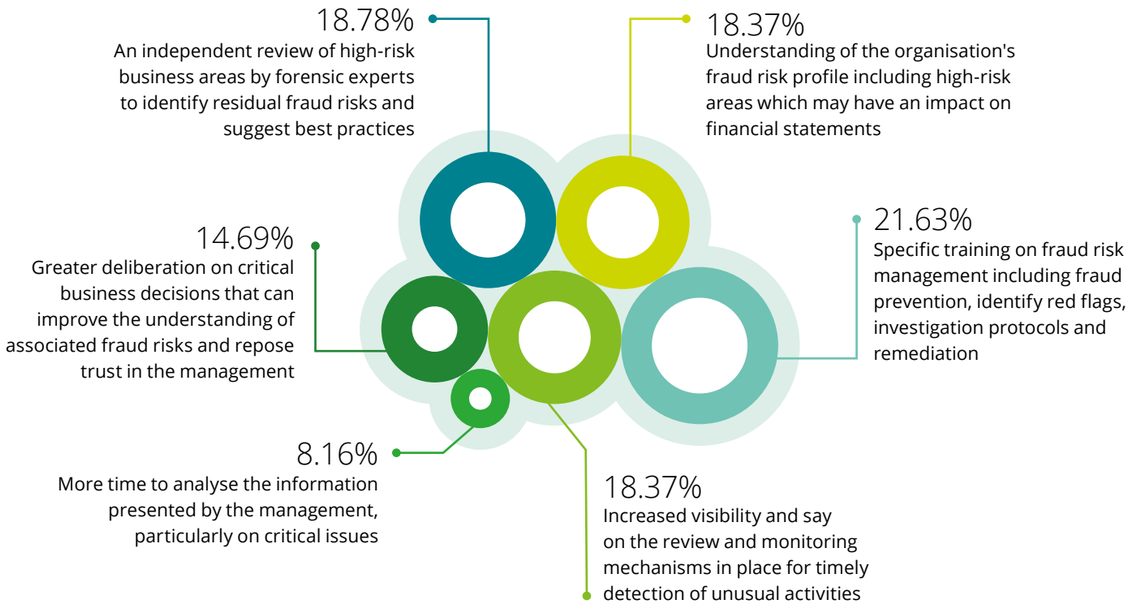
– Around 53 percent IDs believe that they would like to be better equipped to discharge their regulatory and fiduciary responsibilities towards fraud prevention and detection.

Do you believe you are well equipped to discharge your regulatory and fiduciary responsibilities towards fraud prevention and detection? (Select one option in the appropriate category)



– Specific training on FRM (21.63 percent), help from independent experts (18.78 percent) and increased visibility on monitoring protocols (18.37 percent) are the important components that IDs believe will help fulfil their fiduciary responsibilities to mitigate fraud risks.

Which of the following options can better equip you to fulfil your fiduciary responsibilities to mitigate the fraud and misconduct risks? (Select the top three)



Observations

Per the survey results, approximately, 63 percent of the IDs are ready to be part of the board even if they have previously experienced/reported fraud indicating that fraud is no longer a phrase which is taboo. The fact that IDs are willing to associate with organisations with a history of fraud signifies that organisations may at some point witness frauds/ misconduct, however, it is crucial for organisations to improve their fraud risk management efforts across fraud prediction and prevention, as indicated by around 58 percent of the IDs.

Approximately 21 percent IDs felt that a specific focus on increasing awareness amongst employees on ethics, integrity, and reporting fraud or misconduct issues is important to reduce fraud and misconduct. It is pertinent to note that per the ACFE Report to the Nations 2020[3], 43 percent fraud schemes were detected by whistle-blower tips, half of which were tips from employees. This highlights the importance of investing in the education and awareness of employees and business associates on the means and mechanism of fraud/ misconduct reporting. Further, around 16 percent IDs highlighted the importance of focusing on the adoption of advanced technologies in fraud prevention and timely detection of instances of fraud/misconduct. Conducting special audits/reviews of significant or material items impacting financial statements also help the organisation ensure an appropriate financial reporting, as indicated by around 15 percent of the IDs.

While the responsibilities and accountability of IDs have increased manifold in the recent years, the survey findings highlight that around 53 percent IDs believe that they are somewhat equipped to discharge their regulatory and fiduciary responsibilities towards fraud prevention and detection, however, there is a need to better equip IDs to fulfil such fiduciary responsibilities. Further, around 21 percent IDs indicated that conducting specific training for them on FRM (including fraud prevention, identify red flags, investigation protocols and remediation) and around 18 percent indicated that understanding the organisation's fraud risk profile including high-risk areas that may have an impact on financial statements, will help them in effectively discharging their roles and responsibilities. Further, around 19 percent IDs highlighted a need to appoint forensic experts to independently review high-risk business areas to identify residual fraud risks and suggest best practices.

[3] https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf

Key considerations for IDs

Amidst uncertain times that corporates are facing today due to COVID-19, IDs need to act with the highest standards of vigilance and prudence. While the accountability and expectation of IDs in consideration of past corporate scandals/failures have considerably increased over the past few years, regulators are also mindful of the limitation and challenges IDs face as part of their fiduciary responsibilities[4]. In this context, the Ministry of Corporate Affairs ('MCA') issued a clarification on 2 March, 2020[5] mentioning that prosecution proceedings will not be initiated against independent and non-executive directors ('NEDs') unless there is sufficient evidence to prove that such default or violation had been committed with their knowledge or consent or they were guilty of gross and wilful negligence or fraud. To fulfil regulatory obligations and meet stakeholders' expectations, IDs could consider the following measures:

Before joining the organisation

- Evaluate the background and reputation of the management/promoters from a technical capability and integrity standpoint
- Gain an understanding of the fraud risks faced by the organisation after considering industry trends, geo-political factors, macro and micro business trends
- Ascertain the nature of adverse news/media items on the organisation and evaluate the potential risk from a financial and reputational standpoint
- Ascertain the primary elements comprising the organisation's fraud risk governance framework, including steps taken to establish "tone at the top" and mechanisms designed to ensure that employees at all levels understand the organisation's approach to fraud risk
- Review the mechanism implemented by the organisation to communicate and educate the organisation's fraud risk management strategy to all the stakeholders
- Enhance skills/knowledge through training programmes on the emerging fraud risk landscape relevant for the industry and fraud risk management techniques, including best practices to mitigate the risk of fraud

[4] Companies Act, 2013; SEBI Guidelines – LODR, revised listing agreement for stock exchanges
[5] https://mca.gov.in/bin/dms/getdocument?mds=1bTF%252F%252FyAV2xBCubFfIF4YA%253D%253D&type=open

Corporate fraud and misconduct: Role of independent directors

Oversight and continuous monitoring

While the FRM framework implementation responsibility remains with the management, IDs should periodically review and monitor effectiveness of FRM framework. Further, to build a robust FRM framework, IDs should also promote/push the agenda in the board for the senior management to take charge and actively work on the following initiatives:

- Undertaking of periodic detailed assessment of the organisation's risk management system, including a review of the board's capabilities and expertise, considering the industry or regulatory arena in which the organisation operates
- FRM framework knowledge enhancement drives highlighting "best practices" for the board and appointing external consultants to help the board understand and analyse business-specific risks
- Ensuring that the organisation has implemented a well-oiled mechanism to report major or new fraud risks fructified during the period, investigation conducted, and findings are reported back to the board or relevant committees, as appropriate
- Getting comfort on the availability of an approved set of investigation protocols, clearly indicating investigation roles and responsibilities, depending on the nature of an allegation, which helps avoid reputational risks that may arise from inappropriate investigation methods
- Evaluate if the organisation has communicated reporting protocols to be followed by the whistle-blower system operator to notify the designated officials for different types of allegations
- Ascertaining if the organisation has identified in advance, the legal and forensic investigative resources needed to conduct investigation into serious allegations, including the identification of instances requiring support from external subject matter consultants
- Ensuring that the organisation has an adequate system of continuous monitoring in place for critical areas of concern to identify red-flags, if any, on a real-time basis
- Assessing the effectiveness of a continuous monitoring tool to analyse transactions and keep a close look-out for key outcomes and steps taken by the management to tackle potential risks areas
- Performing a review of reports from the statutory auditors, internal auditors, legal counsel, regulators and other experts to understand the risk profile of the organisation and evaluate if the implemented corporate governance framework is robust and sufficiently well-equipped to oversee all facets of the organisation's risk profile
- Scrutinising and challenging high-value complex or "extraordinary" transactions that form a part of financial statements
- Considering all whistle-blower complaints/tips diligently and ensure that the instances of suspected or known fraud is appropriately investigated and suitable action is taken against perpetrators
- Ensuring that the learning from the investigations are considered/incorporated and that the organisation revisited the fraud risk management framework to ensure that loopholes, if any, in the existing anti-fraud controls framework were adequately enhanced to minimise the possibility of reoccurrence
- Promote appointment of independent experts for opinions on key matters

Action items in case of any suspected fraud

In case of any adverse events, IDs should oversee the management response to ensure the effectiveness and provide guidance. Accordingly, below are some of the considerations that IDs should promote:

- Ensuring all the allegations of fraud/misconduct are looked into and acted on by the management
- Ensure that the complexity and severity of the suspected fraud and its implications both from financial, regulatory, and reputation perspective are assessed appropriately
- Ensure that there is a well-equipped team to handle the investigation, fraud incidents are assigned to senior, trusted individuals. Depending on the complexity and potential implications, consider appointing forensic experts to conduct an independent investigation
- Ensure that all efforts are made as an immediate priority for collection and preservation of critical information to avoid any attempt to destruct the evidence/information
- Seeking updates and overseeing the outcome of the investigation to understand the potential impact and any interim action, if required, to be taken by the management, e.g., disclosures to stakeholders, immediate plug for any loopholes, and internal communication

About the survey

This survey report has been developed based on the responses received to a questionnaire that IOD circulated to IDs serving on public company boards across all major sectors in July and August 2021. The survey received around 110 ID responses, out of which about 25 percent held a total experience of more than 10 years as IDs. Around 62 percent IDs serve in listed companies (including listed foreign headquartered companies with India operations) and approximately 38 percent serve in unlisted companies.

The response rate to questions varies; not all respondents have answered all the questions in the survey. Each statistic used in this report is derived from the number of responses to that question and must not be considered consistent across the report.

Contact us

Nikhil Bedi
Partner
Leader, Forensic – Financial Advisory
Deloitte Touche Tohmatsu India LLP
nikhilbedi@deloitte.com

Sumit Makhija
Partner
Forensic – Financial Advisory
Deloitte Touche Tohmatsu India LLP
sumitmakhija@deloitte.com

Rohit Goel
Partner
Forensic – Financial Advisory
Deloitte Touche Tohmatsu India LLP
rogoel@deloitte.com

Tushar Hambir
Director
Forensic – Financial Advisory
Deloitte Touche Tohmatsu India LLP
tuhambir@deloitte.com

Deloitte.