Deloitte.

Bombay Chamber
Bombay Chamber
of Commerce & Industry

De-mystifying fraud risk management
For the board

For private circulation only
March 2015

Helping independent directors and the Board understand and effectively govern fraud risk management practices

Introduction

Organizations today are increasingly concerned about the risk of corporate fraud, given the severe and long lasting legal, economic, and reputational consequences. The Companies Act, 2013, and the revised corporate governance norms of the Securities Exchange Board of India (SEBI) for listed companies, have recognized fraud as a key risk and placed accountability for fraud risk management on the Board of Directors (the Board), audit committee and senior management. In addition, sector regulators are routinely scrutinizing business-specific processes for fraud and malpractice with the intention of curbing them by introducing appropriate legislation/ guidelines.

These developments call for organizations to think strategically and make long term investments to tackle fraud risks in their business operations, and thereby ensure compliance with regulations. However, the Deloitte India Fraud Survey, a research conducted by us recently, indicates that companies tend to follow a largely reactive approach to mitigate fraud. Further, it appears that limited efforts are being made to educate the Board and the senior management on the risk of fraud and the effectiveness of measures currently adopted by organizations.

In the long term, such an approach to manage fraud risks can be unsuccessful. In a fast paced business environment, the nature of fraud risks is constantly changing. Relying on a generic set of dated controls and awareness policies is unlikely to secure the organization adequately from fraud risks. A fraud risk management program that proactively addresses fraud risks is the need of the hour.

For the Board and senior management to formally govern such a program and monitor its effectiveness, there needs to be greater understanding of the fraud risks facing the organization, as well as the gaps in the current measures employed to manage fraud risks.

This document outlines Deloitte India's model to help the Board and senior management ask the right questions to ascertain the organization's current position on fraud risk management and suggest ways to improve its effectiveness.

I would like to thank the Bombay Chamber of Commerce and Industry for partnering with us to release this document. I look forward to your feedback.

Rohit Mahajan
Senior Director and Head
Deloitte Forensic

Foreword

Fraud is today recognized as a business risk and several survey reports indicate that organizations can lose up to 7 percent of their revenues to fraud. The fraud landscape in India is undergoing significant change with globalization, increasing competition, technological development as well as a high degree of aspiration among the working population. While traditional frauds such as theft of goods, and bribery and corruption, continue to thrive, we are hearing cases of new frauds such as phishing, ecommerce fraud, intellectual property theft etc.

To deal with this changing fraud landscape, organizations need to have a robust fraud risk management strategy. To curb the risk of fraud and support organizations in developing a fraud risk management framework, the Companies Act, 2013, has outlined provisions pertaining to fraud risk management. Specifically, it places accountability for fraud on the Board and senior management, including personal liability. This has prompted Independent Directors and senior management executives to re-look at the organization’s fraud risk management practices and find ways to strengthen them – to manage fraud risks better, as well as be compliant with the provisions of the Act.

However, these efforts are not without challenges. Several surveys have shown that Corporate India largely lacks systems and procedures to prevent, detect and respond to fraud in an appropriate manner. For Independent Directors and the senior management to ensure effectiveness of internal controls, a better understanding of fraud risks and existing controls is necessary.

The Bombay Chamber of Commerce and Industry in collaboration with Deloitte Forensic India have drafted a whitepaper that can help Independent Directors and senior management executives take steps towards understanding and improving the effectiveness of their fraud risk management practices. It provides a holistic yet pragmatic perspective of how a senior management professional can drive fraud risk management practices across the organization. Aspects, such as establishing a code of conduct, vigil mechanism, periodic assessment of fraud risks, and fraud control policy, are discussed in this whitepaper.

We are hopeful that this document will help Independent Directors and senior management executives ascertain the effectiveness of their existing fraud risk management practices and find ways for improvement.

I look forward to your feedback and support.

Vikas Gadre
Director General
Bombay Chamber of Commerce & Industry

To question or not - The Board's predicament today

Corporate India today is better sensitized to the risk of fraud and has access to best practices in fraud risk management. Leading Indian companies have dedicated risk management and compliance teams with specific fraud risk management responsibilities assigned to them. These dedicated teams monitor processes and transactions and report their findings annually[1] to the Board and audit committee for review and feedback.

In theory, the measures put in place to mitigate fraud risks and the reporting processes to notify the Board seem adequate. But in reality, how effective are these measures?

Let us consider an example. If the annual fraud risk assessment and compliance report notes less than 2-3 anomalies in transactions in a year, does it indicate a robust fraud risk management process or a poor one? Should the Board accept these results or challenge them?

Our experience indicates that Boards in India don't challenge the outcomes of fraud risk management programs as often as they should. This can be largely attributed to three factors.

a) **Fraud risk is not yet on top of the Board's agenda.** In the past, corporate India has viewed fraud as an unavoidable cost of doing business. Losses due to fraud were considered insignificant to impact the company's financial performance and little importance was given to fraud risk management. However, large corporate frauds unearthed in India over the last decade, have shown that fraud can destabilize companies and bring their operations to a halt. Further, research studies have estimated fraud losses to be worth at least 5 percent of annual revenues[2]. About one-fifth of the respondents to the Deloitte India Fraud Survey conducted in 2014 indicated that they had lost between Rs. 10 Lakh and Rs. 1 Crore to fraud over the last two years. Further, 23 percent said they were unable to quantify fraud losses. Unless the Board and senior management become aware of this reality, fraud risk will continue to be at the bottom of the Board's agenda.

b) **Inordinate reliance on Internal Audit teams to manage fraud risks.** The Board and senior management has traditionally believed that internal audit teams would provide assurance for fraud risk assessment and detection. But this is undergoing a change. Globally, less than 3 percent of frauds are detected via Internal Audit reviews[3]. The majority of frauds are detected through tips, whistleblower hotlines and IT controls. In India too we are observing a rise in the use of these other channels such as whistleblower hotlines and IT controls/ Data Analytics to detect fraud[4]. The Board needs to become aware of these changes and direct the fraud risk management teams to include these measures in the existing fraud risk management program.

c) **Unsure about what constitutes an effective fraud risk management program.** Despite rise in awareness about fraud, it appears that corporate India is still grappling with understanding what could be an effective fraud risk management program for its organization. A majority of respondents to the Deloitte India Fraud Survey indicated 'lack of efficient internal controls and compliance systems' as the top-most reason contributing to fraud. Inability to identify fraud risks and put the necessary safeguards in place could render any fraud risk management program ineffective. Unless the Board periodically questions the effectiveness of existing controls, it cannot propel the organization towards improvement.

While the regulators may be concerned with the mere presence of fraud risk management measures in an organization, the Board needs to focus beyond that and guide the organization towards building effectiveness.

[1] In our experience, while it is preferable to report findings on a quarterly basis, we find that most companies do so annually.

[2] Source: ACFE Report to the Nations on Occupational Fraud and Abuse 2014

[3] Source: ACFE Report to the Nations on Occupational Fraud and Abuse 2014

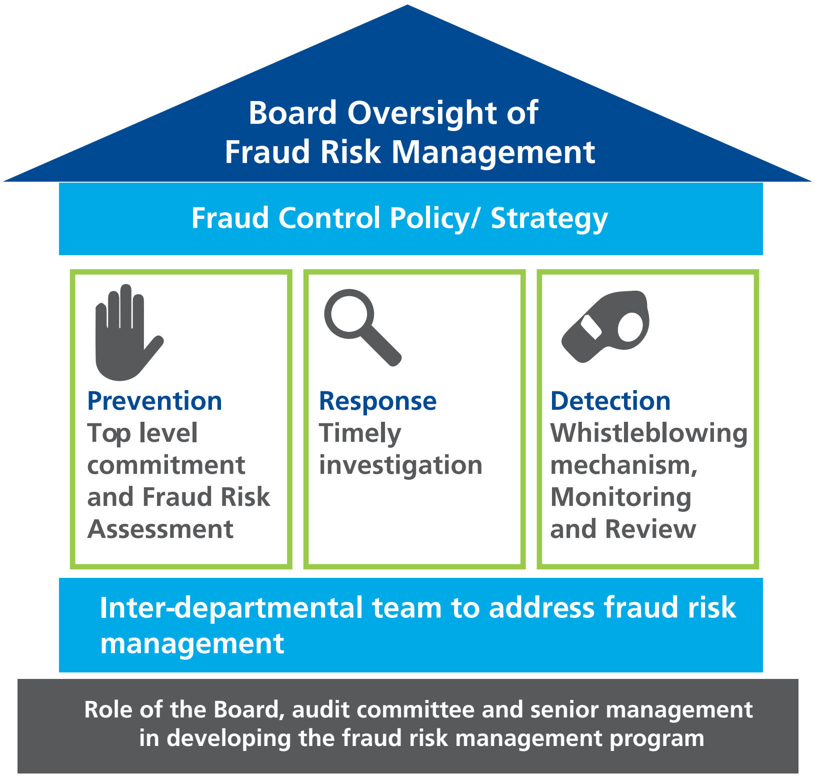
[4] Source: Deloitte India Fraud Survey conducted in 2014

Helping the Board understand and effectively govern fraud risk management practices

A structured approach to fraud risk management can help Boards ask the right questions and understand the organization's outlook on fraud. It can also help set the appropriate agenda for fraud risk management and measure tangible outcomes from the existing program.

Deloitte India's model for fraud risk management involves focusing on identifying and strengthening capabilities across four key areas:

1. The Board's oversight of fraud risk management
2. Role of the Board, audit committee and senior management in developing the fraud risk management program
3. Establishing a formal fraud control policy/ strategy
4. Effective functioning of an inter-departmental team (comprised of key representatives from various departments or functions) to address fraud risk management, and appointing 'fraud risk management champions' to periodically update the Board on the organization's preparedness to understand and mitigate fraud risks


Board Oversight of Fraud Risk Management
Fraud Control Policy/ Strategy
Prevention
Top level commitment and Fraud Risk Assessment
Response
Timely investigation
Detection
Whistleblowing mechanism, Monitoring and Review
Inter-departmental team to address fraud risk management
Role of the Board, audit committee and senior management in developing the fraud risk management program

The Board's oversight of fraud risk management

What is the current state?

The Board and audit committee members have a fiduciary obligation and a corporate responsibility to take steps to prevent, detect, and investigate frauds. Corporate India is aware of the measures necessary to do this and respondents to the Deloitte India Fraud Survey have highlighted some key focus areas[1]: creating a zero tolerance culture, periodic communication to employees on ethical behavior, review of code of conduct to include specific policies on fraud, and sensitizing senior management to the risk of fraud.

However, this awareness does not appear to have translated into action. Boards continue to view these activities at a high level, without understanding how they are implemented across the organization.

What should the Board ensure?

To demonstrate strong oversight of anti-fraud activities, the Board ought to go beyond mere review, to challenge management on the identification of fraud risks and the effectiveness of control activities. The Board also needs to ensure that the organization has implemented an effective ethics and compliance program, and whether that has been periodically tested.

Questions the Board may ask management as a part of its oversight responsibility for fraud risk management, include:

1. How strong is the tone at the top? Does historical evidence of past fraud indicate that unethical behavior will not be tolerated?

2. Are fraud control, prevention and detection policies effectively and regularly communicated throughout the organization, especially for organizations with global operations?

3. Is the whistleblower mechanism effective? What is the frequency and nature of communication sent to employees to build awareness? Are whistleblower reports reviewed periodically to identify red flags and understand patterns and trends, to be presented to the Board?

4. How robust is the company's fraud risk assessment and the assessment of associated controls? How are the findings communicated and addressed?

5. Has the company developed a system for prompt and competent investigation of suspected or known cases of fraud or misconduct?

The Board also needs to encourage an ethical business environment in the organization. This can be done by aligning the rewards system with the core values of the organization. For example, including ethical behavior as part of employee work performance can demonstrate a zero tolerance culture to malpractice and fraud. Further, ethical audits can be initiated to monitor compliance with the code of conduct and ethics policy. Ethical audits can help identify

- Areas where the employee is not getting adequate training about the code of conduct

- Areas where senior management is overlooking suspected/ actual ethical breaches as a result of performance/ result pressures

- Any disconnect between the Board/ senior leadership's stand on ethics, and the practices at various employee levels.

[1] Deloitte India Fraud Survey conducted in 2014

Developing the fraud risk management program - The Board's role

What is the current state?

Formalizing the roles and responsibilities of individuals charged with fraud risk management is the first step towards improving the effectiveness of fraud risk management programs. Although, many organizations have identified ways to implement and improve their current fraud risk management programs, they continue to struggle with capability skill gaps, particularly in the area of investigations, data analytics, and third party due diligence.

What should the Board ensure?

As a part of the fraud risk management plan, the Board can consider the following elements in designing effective fraud risk management processes and encourage ethical behavior among employees and third parties:

1. **Appointing a fraud risk management champion:** Organizations are increasingly appointing champions to oversee critical initiatives. Several multinational organizations have local ethics and compliance champions who translate policy level statements into simple action items to gain employee commitment. On the same lines, Boards can appoint a 'fraud risk management champion' who can periodically appraise them about the effectiveness of fraud risk management processes and controls.

2. **Whistleblower system assessment and benchmarking:** More than 50 percent of all frauds tend to be detected via tips received through whistleblower hotlines . The Companies Act, 2013, specifically mentions the need for a robust vigil mechanism as part of the larger fraud risk management measures to be undertaken by companies. In this context, companies can undertake a benchmarking analysis (against industry specific parameters) to help identify an underperforming whistleblower system, signaling the need for remediation. Often, organizations tend to assume that having few or no disclosures/ calls to the hotline implies that there is little or no wrongdoing going on. Our experience, however, suggests that low call volumes/ disclosures are more likely to indicate opportunities to improve various aspects of the whistle-blower system, including employee awareness. The Board can identify such opportunities for improvement and specifically ask the management for periodic status reports on the remediation efforts.

3. **Comprehensive fraud risk assessment:** Performing an effective fraud risk assessment is the starting point to having an effective fraud risk management program. Conducting periodic employee fraud awareness survey and training can also help identify vulnerabilities and emerging fraud risks. The Board must direct organizations to perform and update its risk assessment regularly to understand evolving fraud risks and the specific vulnerabilities that may apply to the organization over time. An assessment that provides a risk rating (based on evaluation of business processes vis-à-vis their fraud vulnerability and its impact) can be an effective way to periodically evaluate the robustness of anti-fraud control measures.

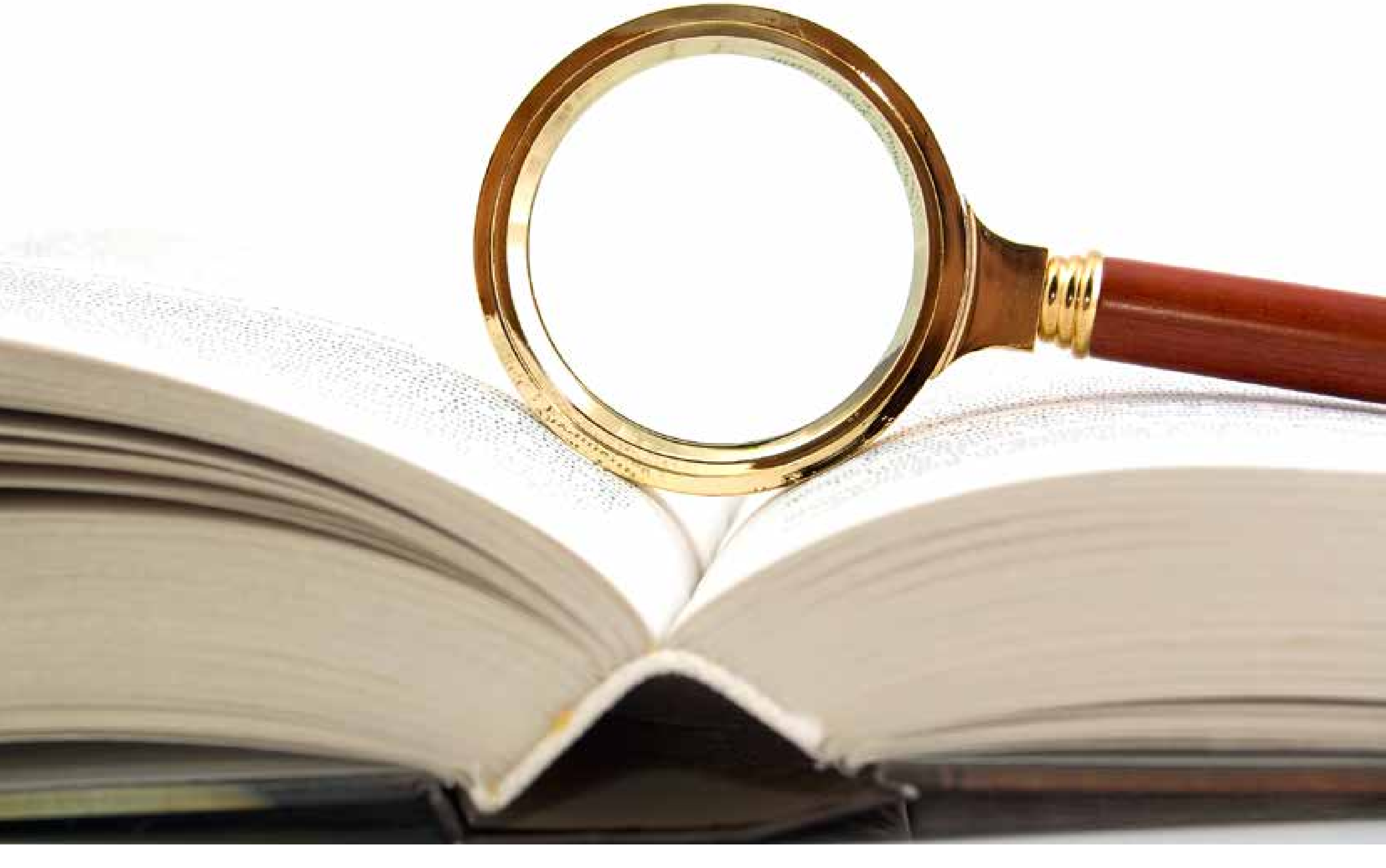
4. **Protocols and resources to manage fraud investigations:** Pre-determining resources and protocols can accelerate the pace of fraud risk management programs and reduce the risk of ineffective investigations. The Board can ask the following questions to the management to ascertain fraud risk management preparedness:
   - Has the company approved a set of investigation protocols to help avoid reputational risks that can arise from inappropriate investigation methods?
   - Has the company communicated reporting protocols to be followed by the whistleblower system operator to notify the designated company officials for different types of allegations?
   - Does the protocol clearly indicate investigation roles and responsibilities depending on the nature of an allegation?
   - Has the company identified in advance, the legal, and forensic investigative resources needed to conduct investigation into serious allegations that may arise wherever the company operates?

Vigilant handling of fraud cases within an organization sends clear signals to the public, stakeholders, and regulators of the Board's and senior management's attitude towards fraud risks and about the organization's fraud risk tolerance.

5. Using data analytics to detect and prevent fraud: Data analytics can be a powerful tool to accelerate the organization's efforts to detect fraud. Data from daily transactions and activities, such as purchasing, accounts payable, sales projections, warehouse movements, employee shift records, etc, can be analyzed to identify patterns indicating potential fraudulent activity. This in turn can help develop appropriate priorities for case management and investigation.

To evaluate the effectiveness of the forensic data analytics technology used by the organization, Boards can ask the following questions:

- Do the data analytics tools used leverage the data within the organization?
- Does the data analytics technology proactively or predictively detect trends prompting further investigation?
- Do employees managing fraud risks know how to use data analytics tools effectively?
- Is the data analytics technology achieving the results you want?



Establishing a formal fraud control policy

What is the current state?

As fraud becomes more prevalent in today's business, having a fraud control policy becomes a critical tool in communicating the organization's stance and processes when confronted with fraud and unethical behavior. Most organizations, in our experience, do not have a formal documented fraud control policy in place. Instances of fraud are dealt on a case basis with significant differences in approach. There is increased reliance on the Code of Business Conduct and Ethics Policy to manage fraud. However, in reality, these documents do not discuss the protocols for tackling fraud.

What should the Board ensure?

A document that sets out responsibilities and procedures to be followed upon the detection of fraud can help organizations take informed decisions. The Board must ask if the organization's fraud control policy includes the following key elements:

1. An explicit definition of fraud and what actions, conduct or behavior constitutes fraud

2. Identifies designated personnel responsible for the overall management of fraud incidents, within and outside the company (including managing the media, regulatory bodies and law enforcement agencies)

3. Formal procedures that employees should follow, in case of suspected or known fraud

4. Encouragement to employees to report concerns about unethical behavior, actual or suspected fraud or violation of the company's code of business conduct and ethics policy

5. A commitment that appropriate measures to deter fraud will be taken, and that instances of suspected or known fraud would be investigated, with suitable action taken against perpetrators

6. A commitment that efforts will be made by the company to recover funds/ assets gained wrongfully by the fraudster and other involved parties.

The fraud control policy must be subjected to a regular review at the Board level.

Effective functioning of an inter-departmental team to address fraud risk management

What is the current state?

Many companies, in our experience, are struggling to determine who will be responsible, to proactively identify fraud risks on an ongoing basis, and manage fraud investigations. The Deloitte India Fraud Survey findings indicate that organizations believe that anti-fraud programs are the responsibility of one designated function alone, such as internal audit or compliance. In reality, this is unlikely given the scope of the activities managed as part of fraud risk management. As a result, confusion can arise, causing a lack of trust amongst management and employees, lack of coordination leading to deficiency in sharing of knowledge, and inefficient response to incidents of fraud.

What should the Board ensure?

An inter-departmental team of key representatives can address fraud risk management efforts on an ongoing basis, and periodically update the Board. On its part, the Board needs to ensure that the team does not face the following challenges that can impede its effectiveness:

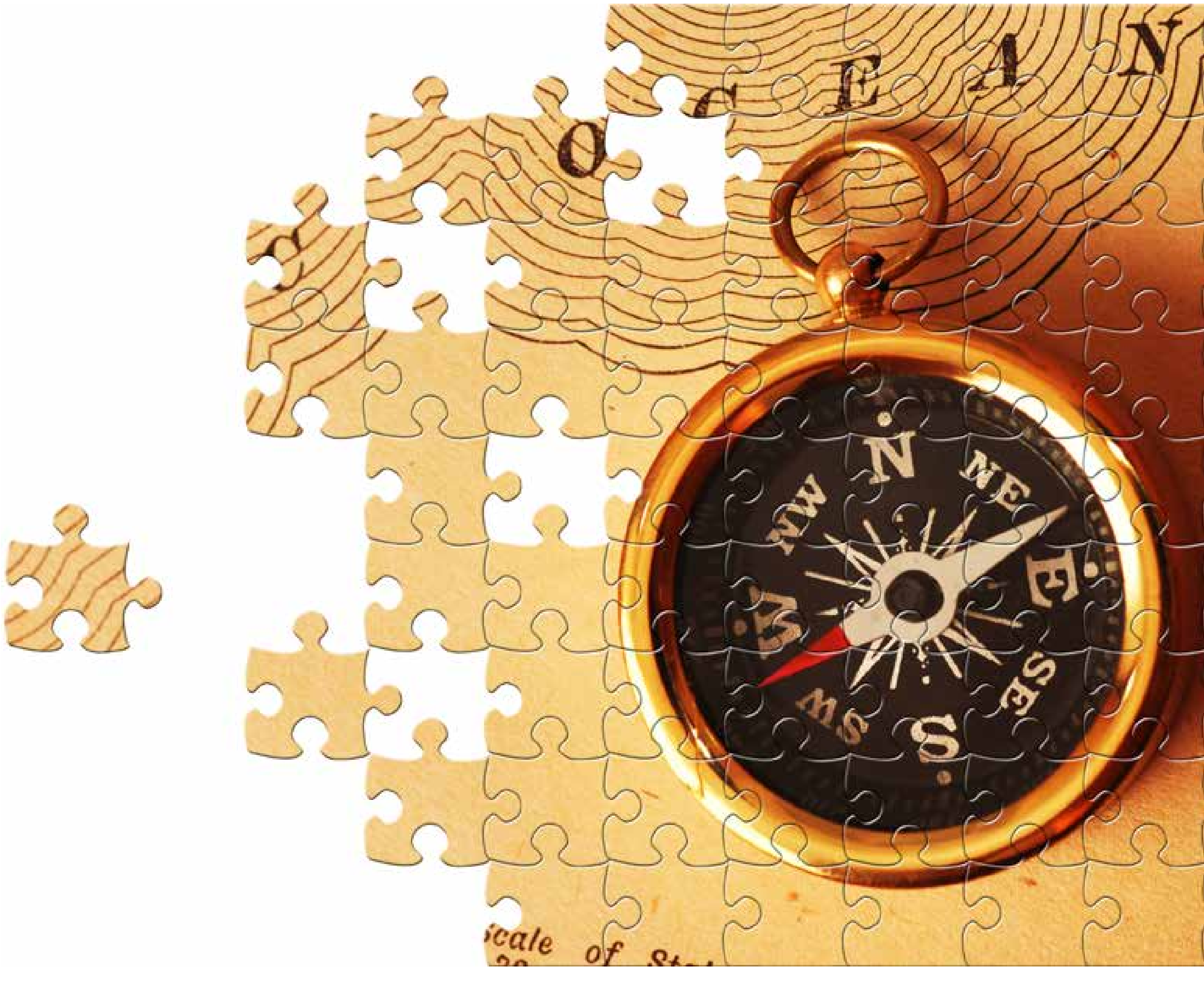
- Lack of clearly defined roles and responsibilities for each team member

- Deficiency in knowledge sharing amongst team members

- Lack of regular training for team members on specific risks, such as those arising from new technologies or business models

Conclusion

The Board and senior management cannot ignore fraud any more, given the personal liability they face under the Companies Act, 2013. To help understand fraud risk management and their organization's preparedness to tackle fraud, Boards must endeavor to question and ascertain facts presented. A structured approach to fraud risk management can be a starting point for Board members wanting to be better involved in their organization's efforts.



Contacts

Rohit Mahajan
Head of Forensic
Tel: +91 22 6185 5180
Email: rmahajan@deloitte.com

Veena Sharma
Director, Forensic
Tel: +91 22 6185 5213
Email: vesharma@deloitte.com

Vikas Gadre
Director General
Bombay Chamber of Commerce & Industry
Tel: +91 22 6120 0202
Email: dg@bombaychamber.com

Important Notice and Disclaimer

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material and the information contained herein prepared by Deloitte Touche Tohmatsu India Private Limited (DTTIPL) is intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). This material contains information sourced from third party sites (external sites). DTTIPL is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such external sites. None of DTTIPL, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this material.