Deloitte.

How prepared is Corporate India to tackle fraud?

An analysis of responses to Deloitte Forensic India's Fraud Risk Score self-assessment tool

August 2016

Forensic

Introduction

Corporate India's efforts in the area of fraud risk management are undergoing a change. This can be attributed in part to greater awareness about the repercussions of fraud as well as enforcement of recent legislations, such as the Companies Act, 2013 and the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015, which mandate companies to have adequate measures to mitigate fraud.

To ascertain how companies were responding to these legislative measures as well as dynamic business changes, we launched a unique web-based initiative in December 2014 – a self-assessment tool (SA tool) that organizations could use to determine their levels of preparedness to tackle fraud, misconduct, and noncompliance. At the end of the assessment, users were given a 'Fraud Risk Score' indicating their preparedness levels, alongside potential areas of improvement, which could be used by them for course correction.

250 C-Level Risk and Compliance professionals undertook the self-assessment in the twelve months succeeding the launch. An analysis of the responses highlight several interesting trends.

While corporate India is becoming more proactive about preventing fraud, enforcement of anti-fraud measures within organizations needs to improve. For example, almost 47 percent of the users who responded to the SA tool indicated that they were still unable to enforce the code of conduct, as employees were not mandated to sign it. Similarly, while companies have invested in technology, such as ERP (Enterprise Resource Planning) platforms and data analytics tools to automate processes and centrally manage them, we observed that over 50 percent of the SA tool users, i.e., those who responded to the SA tool were yet to deploy such technology for fraud risk management measures, restricting themselves to business analysis for now. Further, despite the Companies Act, 2013 mandating the need for a vigil mechanism, around 30 percent of the SA tool users indicated that their organizations did not have a whistleblowing mechanism in place.

Lastly, in the procurement function, a majority of the SA tool users indicated 'mandatory registration of vendors' and 'maintaining comprehensive master data on vendors' as the primary measures taken to prevent fraud. However, only 38 percent highlighted that they reviewed the vendor master data periodically to weed out inactive vendors and only 6 percent of the SA tool users indicated that they performed forensic data analytics on the vendor master data. Further, 49 percent indicated that they did not conduct any due diligence on their vendors.

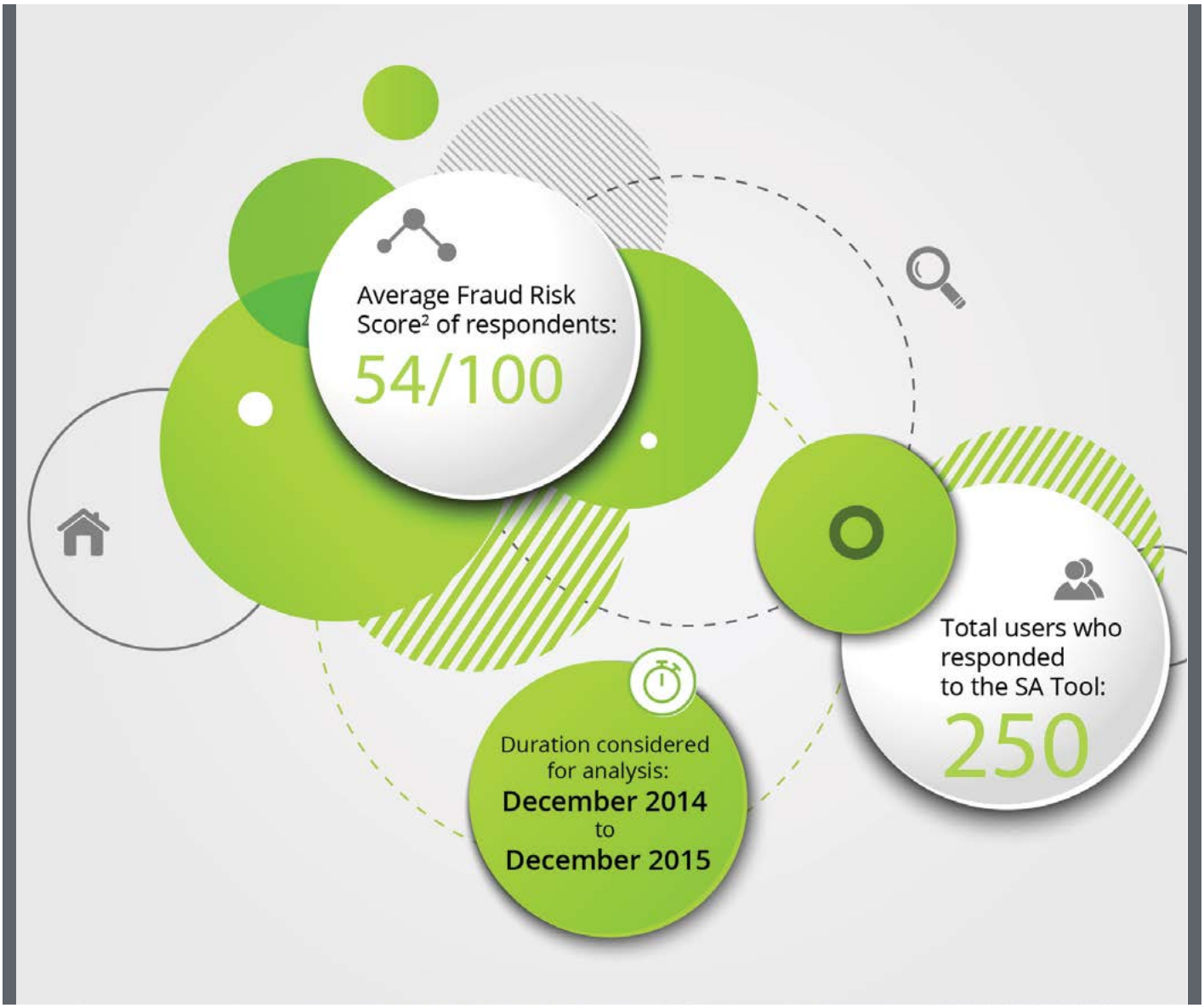
In the area of fraud response, around 60 percent of the users who responded to the SA tool indicated that they were unaware of the presence of a fraud response plan to guide the organization in case any incident arises. With fraud reporting by Auditors mandated as per the Companies Act, 2013, and the recent notification by the Ministry of Corporate Affairs (MCA) prescribing a monetary threshold of INR 1 crore and above for reporting individual cases of fraud to the central government[1], it has become imperative for organizations to establish a fraud response plan.

As the Companies Act, 2013 continues to evolve and provide timely guidance to organizations on aspects of fraud risk management, we expect to see a more structured approach and greater effort from corporate India towards proactively improving their preparedness to tackle fraud. We hope you find this report useful in your efforts to mitigate fraud, noncompliance and misconduct.

Regards
Rohit Mahajan
APAC Leader
Partner and Head – Forensic
Financial Advisory, Deloitte India

1.Ministry of Corporate Affairs (MCA) notification dated 14 December 2015 has amended the rules for 'fraud reporting' stating that if an auditor (of a company) has "reason to believe" that an offence of fraud, which involves or is expected to involve individually an amount of INR 1 crore or above, is being or has been committed against the company by its officers or employees, the auditor should report the matter to the Board or the Audit Committee within 2 days and to the Central Government (after following the due process prescribed for reporting) within 60 days of coming to know about the fraud.

Key Findings



2. The Average Fraud Risk Score has been calculated basis the average figure obtained from all the responses received

Measures taken to prevent fraud:

- 86% of the SA tool users indicated that they had a written code of conduct for employees, but only 53% highlighted that employees were required to sign it annually.
- 75% of the SA tool users have identified people within their organizations who can resolve employee queries on ethical dilemmas and guide them on understanding the code of conduct better.
- 57% of the SA tool users indicated that their organizations did not conduct independent fraud risk assessment of key functions and processes every two years.
- Majority of the SA tool users indicated 'mandatory registration of vendors' and 'maintaining a comprehensive master data on vendors' as the primary measures taken to prevent fraud. Only 38% of the SA tool users highlighted that they reviewed their vendor master data periodically to weed out inactive vendors. However, only 6% of the SA tool users indicated that they performed forensic data analytics on their vendor master data to help analyze the data for potential anomalies.
- Only 51% of the SA tool users indicated conducting due diligence on all vendors. Further, only 30% highlighted that they conducted due diligence on key vendors once a year.

Measures taken to detect fraud:

- Around 37% of the SA tool users indicated that over 75% of their processes were automated and integrated via an ERP system, and managed centrally. Around 19% of the SA tool users indicated that their level of automation was between 50% and 75% and that ERP systems were used to run most processes, alongside the use of data analytics.
- Around 30% of the SA tool users highlighted that they did not have a whistleblower hotline to detect fraud. Another 59% indicated that they had whistleblowing hotlines managed internally.
- SA tool users were divided on the use of data analytics to identify suspicious transactions and other red flags, with 48% saying 'Yes' and 47% saying 'No'.
- Around 54% of the SA tool users indicated that they were able to detect less than 2 instances of fraud in the last financial year.

Measures taken to respond to fraud:

- Close to 60% of the SA tool users indicated that they did not know whether their organizations had a formally documented fraud response plan.
- Among those who responded in the affirmative to having a fraud response plan, the following three components were identified as key aspects in the plan: having an effective system that can receive, manage and track allegations (51%); assigning of the matter to the appropriate and independent party for investigation in accordance with established roles and responsibilities (45%); execution of the actual investigation steps based upon existing guidelines, policies, and procedures that follow well-designed protocols and legal guidance, as appropriate (45%).

Call to action

Improving preparedness to prevent, detect and respond to fraud

Having an enforceable code of conduct: Around 86 percent of the SA tool users indicated that they had a written code of conduct for employees, but only 56 percent highlighted that employees were required to sign it every year. This can result in limited commitment and subsequently limited compliance with the code by employees. As a good practice, the code of conduct should ideally be reviewed every year in keeping with business dynamics and legislative changes and employees should undergo trainings, including signing a declaration as an affirmation of acceptance to the code of conduct when doing business for and on behalf of the company. To improve compliance with the code of conduct the following measures may be considered:

- Designating an 'ethics champion' who can resolve employee queries on ethical dilemmas and help them understand the code of conduct better.
- Include ethical behavior assessment as a component of the overall performance appraisal cycle, giving an opportunity to reinforce the message.
- Link the completion of code of conduct related training with disbursal of compensation. In our experience, some organizations tend to withhold pay until such trainings have been completed.

Undertaking a fraud risk assessment: Around 57 percent of the SA tool users indicated that their organizations did not conduct independent fraud risk assessment of their key processes every two years. 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. In our experience, some of the suggested processes that should be regularly reviewed as part of an ongoing Fraud Risk Management (FRM) are:

- Sale (order to cash) process - bidding, client onboarding, customer master management, sales order creation, billing to the client, revenue recognition and accounting, and collection from the customer
- Procurement (procure to pay) process - vendor selection and onboarding, purchase of goods/ services (approving purchase requisitions, raising purchase orders, etc.), goods/ services receipt, invoicing, vendor advances and reconciliations
- Human Resources (HR) (hire to retire) process – candidate selection, recruitment, employee master, attendance and payroll processing
- Financial reporting and closing (record to report) process
- Treasury, involving cash, bank operations, corporate investments and borrowings
- Employee expense reimbursement claims process

Re-looking at vendor management practices: The majority of the SA tool users indicated 'mandatory registration of vendors' and 'maintaining comprehensive master data on vendors' as the primary measures taken to prevent fraud. However, only 38 percent of the SA tool users indicated that they cleaned up/ reviewed their vendor master data periodically to weed out inactive vendors. Further, only 6 percent of the SA tool users highlighted that they performed forensic data analytics on their vendor master data. While these statistics indicate that organizations are digitizing vendor records, this activity in itself is not related to fraud risk management. In our experience fraud risks involving vendors tend to exist despite the presence of digital records. Therefore, organizations need to focus on the 'next level' of action(s) that should be performed on the vendor data. These can include:

- Three-way match to ascertain whether vendor payments are genuine.
- Determine whether there is a conflict of interest with other vendors in the system or with employees.
- Conduct a due diligence on vendors – Only 51 percent of the SA tool users indicated conducting due diligence on all vendors at the time of onboarding. Further, only 30 percent indicated that they conducted due diligence on key vendors once a year. In a fast growing economy like India, vendors too tend to outgrow the services they may have initially provided to organizations. To inadvertently prevent situations such as conflict of interest and bribery and corruption risks, it is necessary to conduct periodic due diligence on the following vendor aspects:
  - Ascertaining whether a vendor exists in reality, the ownership pattern and incorporation details
  - Vendor capabilities (infrastructure and resources, to name a few) to deliver on the job bid for/ specified
  - Links with political parties/ representatives or government officials
  - Reputation of any litigation history pertaining to patent infringement, counterfeiting, bankruptcy, child labor or product safety issues
  - Association with known/ suspected corrupt activities/ terrorist groups

Segregation of duties, particularly in the procurement function, is also a key aspect that can prevent vendor related fraud risks. Around 36 percent of the SA tool users indicated that there was no segregation of duties ("SOD") in their organization in the Accounts and Finance department for recording and processing of transactions related to income, expenses, assets and liabilities. The lack of SOD can provide an opportunity for employees to commit fraud or conceal fraudulent activity.

Leveraging technology to detect fraud: The level of automation and evidence trail provided by technology can make it difficult to conceal fraud. However, organizations appear divided on the use of technology and data analytics tools to identify suspicious transactions and other red flags (47 percent agree, while 48 percent disagree). In our experience, the success of detecting potential fraud using technology and data analytics requires the following considerations:

- The quality of data present – An incomplete vendor master file would be unlikely to yield significant results when analyzed. Similarly, outdated information may result in misleading outcomes when put through a data analytics program. It is therefore important that organizations keep their data up to date and comprehensive.
- The technology platform used to leverage data – Any technology platform can help host organizational data. While some technology platforms come with inbuilt modules that are customized to support certain applications like payroll, or accounts payables, others may require additional customization. Organizations therefore need to make a conscious decision about their requirements by considering aspects such as scale of data, key processes to be monitored, level of investment in technology, etc.
- Customization and use of data analytics tools - Around 54 percent of the SA tool users indicated that they were able to detect less than 2 instances of fraud in the last financial year. This can often happen because the right data sets may not have been used for analysis. For example, in order to identify potential undisclosed relationships between employees and vendors analyzing the employee and vendor database would be beneficial; whilst to identify anomalies in purchasing the accounts payable data would be appropriate. Some examples of anomaly/ unusual pattern detection tests that can be employed include:
  - Common bank account, address, and phone numbers between vendors and employees that may indicate a potential conflict of interest
  - Payment to terminated or suspended or fictitious vendors
  - Duplicate payment to vendor against invoices with the same amount, date and invoice number
  - Multiple payments relating to the same requisitions, order numbers or invoices
- Ability to understand reports/ dashboards - Forensic data analysis can, for example, highlight unusual patterns/ trends in data, such as the number of invoices from suppliers/ vendors over time, unusual invoice number sequencing, and unusual amounts spent for goods and services purchased from a particular vendor. Organizations need to delve deeper by asking questions such as "does the amount spent and timing of purchases from a particular vendor make sense?" or "does the price paid for the goods and services make sense?"
- Deciding the response to reports/ dashboards – Organizations can often tend to dismiss red flags as one time anomalies. However, this may not always be the best response. Take the case of a multinational that we worked with. A forensic data analysis of purchases by the maintenance department revealed that the price paid for various supplies was two and sometimes three times higher than the market value. Investigating these anomalies revealed a connection between the vendor and maintenance department procurement officer.

Over time, technology platforms can also be extended to include other channels of detecting fraud such as whistleblowing. A tip off received via a whistleblowing channel can help companies compare the suspected activity with past data relating to red flags for evidence. For example, a whistleblower working at a large manufacturing unit alleged that an employee in the procurement department was in collusion with a vendor to bill the company for security services that were allegedly never rendered. An investigation performed using forensic data analytics tool of the accounts payable data over the last five years revealed several large round amount invoices billed for security at events that the company had no record of having organized (i.e., fictitious invoices were recorded). This scheme appeared to have lasted for several years and cost the company significantly.

Drafting and operationalizing a fraud response plan: Close to 60 percent of the users that responded to the SA tool indicated that they were unaware if their organization had a formally documented fraud response plan. A fraud response plan ensures that incidents are handled in a systematic and efficient manner, not only to conclude a successful investigation, but also to demonstrate that the organization acted in a prudent and lawful manner. A fraud response management plan should ideally:

- Identify a committee/ specific team to whom the incident is escalated to/ informed.
- Include defined roles and responsibilities/ accountability of who (within the firm) handles a fraud incident/ allegation when it comes to light.
- Keep legal considerations in mind w.r.t. who gets involved and who takes care of investigative and regulatory aspects (including protection of documentation and evidentiary procedures)
- Define investigation protocols/ the action that needs to be taken following detection of an incident of fraud. For example:
  - Identify competent fraud investigation resources, prior to a crisis, especially if a global response team is required.
  - Identify the methods and procedures by which allegations are to be investigated.
  - Outline the scenarios that call for third party expertise
- Include effective and consistent communication protocols in order to manage employees within the firm as well as externally across varied stakeholders such as regulators, the media etc.
- Include remediation recommendations related to understanding the root cause of the occurrence of the fraud incident as well as accountability of a team/ individual for implementation of the recommendations/ remedial measures to help prevent recurrence.

In our experience, having a well-documented fraud response plan is just the starting point in order to respond to fraud. It needs to be backed by successful implementation. We have observed that organizations often lack adequate fraud investigation resources and technology to gather information and investigate an incident. These aspects are as important, if not more, to successfully detect and report fraud.

Conclusion

Corporate India has work to do when it comes to tackling the menace of fraud, as observed from all the responses collated. Additionally, with the increasing use of technology in business, the emergence of new frauds, including cyber-crime, requires organizations to be well-informed of the fraud vulnerabilities in their business processes, concurrently requiring them to build robust fraud risk management practices.

In an era of intense scrutiny from regulatory agencies, with recent increasing cases of formal, regulatory action and investigation initiated by regulators, organizations need to necessarily understand what steps to take in order to be compliant and deter fraud incidents from erupting. While policies and procedures pertaining to fraud risk mitigation are important, it is equally important to understand that without the ability to operationalize these policies and procedures, preventing fraud is not possible. This is also the message that is being driven by key legislations such as the Companies Act, 2013 (the "Act"). The Act prescribes guidelines on fraud risk management, but expects that companies would operationalize these efforts on their own, in line with the unique fraud risks that their businesses are susceptible to. This trend thus raises the stakes for those charged with governance.

Key contacts

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

Veena Sharma
Director
Forensic – Financial Advisory
Deloitte India
T: +91 22 6185 5213
E: vesharma@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.

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 is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. Without limiting the generality of this notice and terms of use, nothing in this material or information comprises legal advice or services (you should consult a legal practitioner for these). None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should consult a relevant professional for these kind of services. This material or 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 or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.

©2016 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited

Deloitte Touche Tohmatsu India Private Limited (U74140MH199 5PTC093339) a private company limited by shares was converted into Deloitte Touche Tohmatsu India LLP, a limited liability partnership (LLP Identification No. AAE-8458) with effect from October 1, 2015.