Deloitte.

Building effective internal financial controls for better fraud risk management

June 2015
www.deloitte.com/in

A Point of View

The Companies Act, 2013 (the "Act"), is perhaps the first legislation of its kind in India to place explicit emphasis on the need for robust Internal Financial Controls ("IFCs") [1] to address the risk of fraud. However, there is limited guidance in the Act on aligning IFCs towards better fraud risk management, leaving companies to come up with their own practices to measure and address the risk of fraud. In our view, this can be a challenge for companies whose ability to deal with fraud can be limited by resources, awareness and skilled personnel.[2]

We observe that several leading companies are adopting well known frameworks, such as the Committee of Sponsoring Organizations of the Treadway Commission 2013 – Internal Control Integrated Framework [3] ("COSO 2013 Framework"), to develop their IFCs. Originally developed for the U.S. market to enable compliance with the Sarbanes Oxley Act, the COSO 2013 Framework covers internal controls from a 360 degree view, emphasizing on the need for organizations to perform ongoing and/or separate evaluations to ascertain whether the internal controls exist and are operating. Specifically on fraud risk management, the COSO 2013 Framework (under Principle 8) suggests that companies 'Asses Fraud Risk,' including the risk of bribery and corruption, separate from the general risk assessment that is otherwise undertaken.

1 Source: http://thefirm.moneycontrol.com/story_page.php?autono=1392421

2 Source: The Deloitte India Fraud Survey 2014, indicates that over 80 percent of survey respondents experienced fraud. A large number of respondents also mentioned facing challenges with clarity around internal controls specific to issues such as bribery and corruption and availability of skilled resources to manage forensic technology.

3 Source: http://www.coso.org/IC.htm

Our observation is that this is easier said than done, given the challenges that companies face while building a fraud risk management program. Some of the common challenges observed by us include:

Inability to perform an effective fraud risk assessment

Organizations' focus on risk assessment usually tends to be more on general operational risks, regulatory risks and financial reporting risks, rather than fraud risks. This can make it difficult to view fraud in isolation and consider industry specific risks and potential fraud schemes as part of the fraud risk assessment.

Ineffective segregation of duties

Failure to segregate duties appropriately across multiple systems/ manual processes can inadvertently allow employees to commit fraud or conceal fraudulent activity. For instance, there could be cases where password sharing (for gaining access to system/ financial transactions) amongst a group of people has diluted internal controls, leading to fraud.

Limited monitoring of third parties

Most companies do not communicate their organization's expectations of integrity and ethical values to third parties. Further, despite the fraud risks posed by third party actions (such bribery/ corruption), there is limited monitoring of their activities. Contract clauses are often not stringently enforced and due diligence practices undertaken are not comprehensive.

Limited ability to demonstrate ethical behavior or compliance with an ethics program

Although organizations have established ethics programs, they may not always evaluate the effectiveness or tangible impact created through such programs. Also, many times, the pressure to meet targets and actions of senior management may tacitly encourage employees to overpower/ violate the organization's message on integrity and ethical values. Such instances fail to demonstrate compliance with the ethics program.

The challenges listed above indicate the need for a pragmatic fraud risk management program that organizations can implement backed by robust internal controls.

Building a pragmatic fraud risk management program

A pragmatic fraud risk management program can benefit companies by identifying potential fraud in advance and help plug the necessary gaps in their endeavor to build an effective internal financial controls environment. Deloitte India's recommended model for building IFCs targeted to mitigate fraud risks focuses on four key components –

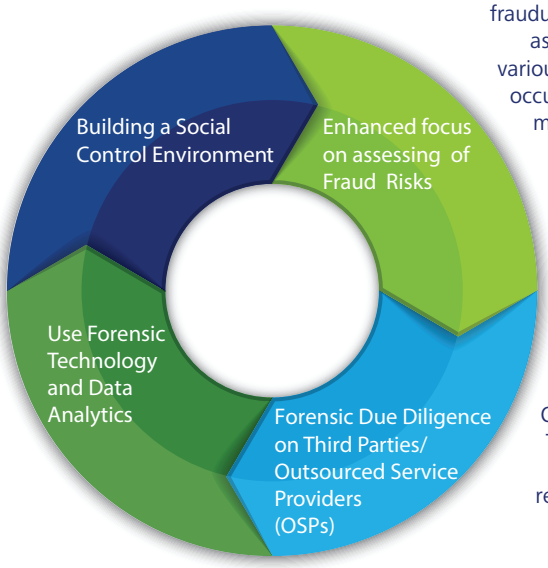
1. Building a social control environment, through fraud awareness/ ethics surveys, trainings, etc.
2. Enhanced focus on consideration of fraud risks
3. Use of forensic technology and data analytics
4. Forensic due diligence on third parties/ Outsourced Service Providers (OSPs)

Each of these aspects is discussed in detail in the following pages.

The Deloitte India model for building IFCs to mitigate fraud

Fraud and Ethics Survey or Ethical Dilemma Workshops
Culture is a good barometer for measuring an organization's susceptibility to fraud. Understanding an organization's culture is fundamental to designing effective antifraud controls, as there is a strong correlation between an organization's ethics and culture and its vulnerability to fraud.
Fraud and ethics survey help directors and management accurately assess, understand and strengthen the ethics and culture of an organization (and in doing so help manage their fraud risk).

Forensic Technology and Data Analytics
Entities with multiple lines of businesses, often operate fragmented IT systems. The Board of directors need to understand an organization's data integrity and its preparedness towards cyber threat and vulnerability.



Enhanced focus on Assessing Fraud Risks
Entities must consider the potential for fraud in performing risk assessments. The assessment of fraud must consider fraudulent financial reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur. The board of directors must oversee management's assessment of fraud risks.

Third Party/ Vendor Due Diligence
As entities increase their reliance on OSPs, greater attention and oversight of Third-party Vendor Risk Management is required to manage the integrity and reputation risks arising due to fraudulent activities by the third party.

Building a social control environment

Diminishing ethical values and lack of a robust code of conduct within the organization have been identified as key reasons for fraud, according to respondents of the Deloitte India Fraud Survey, released in 2014. Further, senior management was considered the most susceptible to commit fraud, as per the survey respondents. These factors highlight the need for a strong ethical culture and social control environment within the organization to tackle fraud. Some of the following measures can, over time, help develop an ethical enterprise.

Areas of focus	Specific measures to consider
Code of conduct	• Ensure that new employees acknowledge the code of conduct and accept to abide by it. • Seek employee acknowledgment and acceptance every time the code is revised. • Ensure that third parties acknowledge the code of conduct proportionate to the scope of their operations. • Undertake review of the code of conduct periodically (the leading practice is to review it annually). • Ensure that policies are worded in simple language without ambiguity. • Include specific clauses pertaining to fraud. • Form an internal team that researches on new frauds and communicates that to the organization. • Revise the policy in line with the changing fraud risk landscape. eg. fraud risks from social media use by employees can be specifically stated.
Establish a whistleblowing system	• Provide multichannel / multi-lingual access to the system for all employees and third parties, encouraging them to report unethical behavior, fraud or misconduct. • Maintain records of all the disclosures made by employees and external parties. • Periodically evaluate the system for its effectiveness in terms of industry bench-marking analysis, awareness amongst employees, other stakeholder communication, and integration with other ethics program.
Develop an anti-fraud policy	• Clearly list various protocols for reporting unethical behavior related to fraud, misconduct or fraudulent financial reporting. • Evaluate and investigate unethical behavior and violations of the code of conduct on time. • Avoid censoring information received by the board on whistleblowing incidents.

Areas of focus	Specific measures to consider
Align rewards system with core values	• Include ethical behavior as a key component of employee performance appraisal. • Recognize, celebrate and incentivize (if necessary) ethical behavior. • Allow discussion of difficult, controversial or sensitive matters with senior management.
Undertake ethical internal reviews to monitor compliance with the Code of Conduct	• Management can evaluate trends in the volume or nature of unethical behavior reported and determine whether to take steps to improve actions regarding the ethics program. • Management can perform periodic ethics assessments, including third-party ethics internal reviews.
Training/ awareness programs, workshops and surveys	• Conduct fraud and ethics survey to understand disconnects between the leadership's tone at the top versus the activities at the ground level. • Build awareness on fraud trends, damage due to fraud and practical scenarios that fraud can manifest itself in. • Conduct ethical dilemma workshops for employees for identifying emerging issues. • Use a range of media – video, events, online chat, blogs etc. – to communicate with employees on anti-fraud measures.

Enhanced focus on the consideration of fraud risks

A recent Deloitte – BCCI whitepaper titled *De-mystifying fraud risk management for the Board*, released in March 2015, highlights the challenges faced by senior management and the Board in understanding fraud. The whitepaper highlights the following aspects:

- Fraud risk is not considered top of the Board's agenda due to the perceived low cost of losses due to fraud;
- Inordinate reliance on internal audit teams to tackle fraud risks;
- Limited understanding of what constitutes an effective fraud risk management program.

These challenges can impact the manner in which the fraud risk management program and its corresponding IFCs are developed. Companies therefore need to re-look at their fraud risk assessment processes. The table below highlights some of the key aspects which we have observed companies overlook while undertaking a fraud risk assessment. Addressing these areas can help build a strong foundation of IFCs better aligned to the fraud risk management program.

Areas of focus	Specific measures to consider
Assess the types of frauds that can impact business	Consider relevant types of fraud, such as fraudulent financial reporting, possible loss of assets, and corruption schemes through which fraud and misconduct can occur.
Consider ways that fraud can occur	Some of the factors to be considered, include: • Management bias (e.g., in the selection of accounting principles) • Degree of estimates and judgments in external reporting • Vulnerability to management override and potential schemes to circumvent existing control activities • Understanding bribery and corruption risks • Geographic regions, where the entity does business, and prevalent fraud risks in that region • Incentives that may motivate fraudulent behavior (e.g., identifying the entity's fraud risks, particularly when earnings pressures and aggressive incentive compensation programs exist) • Nature of technology and management's ability to manipulate information • Unusual or complex transactions subject to significant management influence
Address fraud risks in light of changes in the operating environment	Re-evaluate fraud risks as and when there are changes in the entity or external environment, such as regulatory changes or business environment.
Understand fraud risks through business partners	Assess the manner in which work is performed by vendors, outsourced agencies and other third parties doing business for and on behalf of the company.
Review results of the fraud risk assessment undertaken	Periodically review the results of the fraud risk assessment with the audit committee, and challenge the findings of the assessment for aspects, such as management override of controls.

Use of forensic technology and data analytics

Forensic technology and data analytics used for fraud risk management can significantly improve fraud identification and detection outcomes. Respondents to the Deloitte India Fraud Survey, released in 2014, have identified at least 11 types of frauds that can be detected using forensic technology and data analytics.

Source: Deloitte India Fraud Survey, Edition I, 2014

Despite the rise in awareness about the use of technology in fraud mitigation, a majority of respondents to the Deloitte India Fraud Survey, released in 2014, indicated facing multiple challenges in using forensic technology and data analytics:

- Lack of skilled resources to manage data analytics roles on a daily basis;
- Lack of awareness around using forensic data analytics proactively in fraud monitoring;
- Perceived high cost of software installation and management;
- General lack of knowledge among decision makers on the use of data analytics;
- Poor data quality which may render forensic data analysis ineffective.

Rather than invest heavily in forensic technology, it is recommend that companies start their efforts in leveraging technology by re-aligning their existing technology controls to detect and prevent fraud [4]. The below table highlights six key aspects that companies can consider to kick start their technology efforts .[5]

Areas of focus	Specific measures to consider
Proactively monitoring key processes	Run data analytics modules on internal/ external communication, payroll and reimbursements, receivables and collections, sales and distribution, time and physical access controls, vendor payments.
Logging and maintaining an audit trail of activities	• Develop a robust log maintenance policy • Determine retention period of logs in line with fraud risk management requirements • Run analytics routinely on logs
Automated notifications in case of process over rides	Designated stakeholders can receive automated messages in case of any incidents.
Active threat monitoring and management	Enable cross departmental integration of data from systems such as HR, Finance, payroll and administration to get a holistic view of fraud risk management.
Audio visual monitoring	Integrate video feed with ERP data to cross check details pertaining to transactions.
Data leakage prevention software	• Periodically relook at key words and refresh them • Tweak policy on emails that restrict certain types of emails going to/from a specific ID
Adequate control on devices containing confidential data	• Encrypt devices • Use software tools with remote data wiping capabilities to safeguard against device theft or intrusions

4 In case, some of the basic technology infrastructure is not already in place within an organization, then it is recommended that companies start investing in technology controls in those areas identified as 'high risk' to reduce fraud vulnerabilities.

5 Source: The Deloitte India Fraud Survey, released in 2014

Forensic due diligence on third parties and outsourced service providers (OSPs)

Working with third parties can significantly increase the risk of fraud [6]. It is observed that, Indian companies are able to extend limited control over their third party ecosystems and unlike some of the other countries, incorporating right to audit clauses in vendor contracts may be perceived as a breach of trust, damaging the business relationship. In these circumstances a forensic due diligence can be a useful tool to understand one's vendors and other business partners. The following table, based on our observation of the Indian market, lists the areas of focus to be covered by a forensic due diligence on Third Parties/ Outsourced Service Providers (OSPs) in order to address related fraud risks.

Areas of focus	Specific measures to consider
Knowledge of third party background information, including ultimate beneficial ownership (UBO) and affiliates	• Experience and competence/track record • Are these fronts/shell companies for money laundering? • Collusion with employees • Clients and other business relationships
Business interests/ affiliations	Conflict of interest
Adverse media	• Evidence of past or current corruption • Unethical business practices • Involvement in tax evasion • Involvement in terrorist financing • Links to organized crime • Involvement in money laundering • Other reputational issues
Litigation history	Involvement in legal proceedings/ convictions for malpractice/ crime etc
Political affiliations	Inappropriate political support and links to politically exposed persons / entities.
Sanctions/ high risk entities	• Business operations in Office of Foreign Assets Control (OFAC) sanctioned countries • Other reputational concerns
Regulatory screening	Action by competent authority for lapses or defaults
Financial position screening	• Financial position snapshot • Historic analysis of Financial position • Financial capacity to execute commitments
Credit history	Credit defaults and bankruptcies

6 Source: The Deloitte India Fraud Survey, released in 2014

Conclusion

The Companies Act, 2013, provisions have prompted organizations to re-look at their fraud risk management efforts. While organizations have taken some steps towards mitigating the risk of fraud, more can be done to develop internal financial controls that can effectively address the risk of fraud, in light of the fast changing regulatory and business environment.

The Deloitte India model for developing financial controls is pragmatic and provides some leading practices that can help organizations to manage fraud risks, through the development of a holistic and a structured fraud risk management framework.

Companies that can build the right social control environment, enhance focus on assessing fraud risks, proactively use forensic technology and data analytics tools, and implement third party due diligence procedures can accelerate their efforts in implementing a holistic fraud risk management framework in line with the expectations of the Companies Act, 2013.

Contact Us

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

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

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

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

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

Veena Sharma
Director
Forensic – Financial Advisory
Deloitte in India
Tel: +91 22 6185 5213
Email: vesharma@deloitte.com

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

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


HIGH
MED
LOW

Important Notice and Disclaimer

This document is provided as general information only. This document and the information contained herein prepared by Touche Tohmatsu India Private Limited ("DTTIPL" or "Deloitte India") is intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). None of DTTIPL, Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its member firms, or their related entities (collectively referred to as "Deloitte Network") is, by means of this document, rendering professional advice or services.

DTTIPL do not express an opinion or any other form of assurance. Further, comments in this document are not intended, nor should they be interpreted to be legal advice or opinion.

- This document contains DTTIPL analysis of secondary sources of published information and may incorporate the inputs gathered through meetings with various industry experts and other industry sources, which for reasons of confidentiality, cannot be quoted in this document. DTTIPL does not undertake responsibility in any way whatsoever to any person or entity in respect of errors in this document, arising from incorrect information provided by the industry experts and/or other industry sources.
- While information obtained from the public domain has not been verified for authenticity, DTTIPL have endeavored to obtain information from sources generally considered to be reliable. DTTIPL assume no responsibility for such information.
- DTTIPL's analysis (if any) in the document is based on the prevailing market conditions and regulatory environment and any change may impact the outcome of DTTIPL' analysis. Further, such analysis indicates only that DTTIPL have undertaken certain analytical activities on the underlying data to arrive at the information presented; DTTIPL do not accept responsibility or liability for the underlying data.
- DTTIPL must emphasize that the realization of the benefits accruing out of the recommendations set out within this document (based on secondary sources, as well as DTTIPL internal analysis [if any]), is dependent on the continuing validity of the assumptions on which it is based. The assumptions will need to be reviewed and revised to reflect such changes in business trends, regulatory requirements or the direction of the business as further clarity emerges. DTTIPL accepts no responsibility for the realization of the projected benefits. DTTIPL's inferences therefore will not and cannot be directed to provide any assurance about the achievability of the projections. Since the projections relate to the future, actual results are likely to be different from those shown in the prospective projected benefits because events and circumstances frequently do not occur as expected, and differences may be material. Any advice, opinion and/ or recommendation indicated in this document shall not amount to any form of guarantee that DTTIPL has determined and/ or predicted future events or circumstances.
- DTTIPL's views are not binding on any person, entity, authority or court, and hence, no assurance is given that a position contrary to the opinions expressed herein will not be asserted by any person, entity, authority and/or sustained by an appellate authority or a court of law.

DTTIPL will not be liable for any direct, indirect, incidental, consequential, punitive or other damages, whether in an action of contract, statute, tort (including without limitation, negligence) or otherwise, relating to the use of the analysis and information contained herein.

Deloitte refers to one or more of 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. DTTIPL is a member firm of Deloitte Touche Tohmatsu Limited.

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

By reading the document the reader of the document shall be deemed to have accepted the terms mentioned hereinabove.

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. 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 seek specific advice of the relevant professional(s) 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.

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.