Deloitte.

Implementing a robust fraud risk management program

10 Frequently Asked Questions

Understanding Fraud Risk Management

1 Are there any specific forensic audit requirements listed in the Companies Act, 2013? What are the corresponding penalties for noncompliance or failure to prevent fraud?

Although the Companies Act, 2013, explicitly states the need for establishing risk management systems to prevent and detect fraud, there is no specific framework or guidance provided by the Companies Act, 2013 on conducting a forensic audit. Companies are expected to devise practices to measure and address the risk of fraud depending upon the nature, operating industry and size of the business, among other factors. A forensic audit may help companies understand their vulnerability to fraud.

Section 447 of the Companies Act, 2013, deals with provisions relating to penalties for fraud, including acts related to the failure by companies to establish risk management systems to prevent and detect fraud. The punishment covers directors, key managerial personnel, auditors and/or officers of the company and goes beyond professional liability for fraud, extending to personal liability in case of noncompliance.

2 Apart from internal audit and whistle-blowing, what other mechanisms can help the management in tackling fraud?

The three primary processes that a fraud risk management framework should include are: regular monitoring/ assessment of fraud risks, conducting due diligence checks on counter parties, and the use of proactive data analytics to review transactions for red flags/ anomalies/ gaps in internal controls, according to the Deloitte India Fraud Survey, released in 2014.

Due diligence involves conducting background checks on the counter party to assess the veracity of their claims (pertaining to capabilities, financials, key business personnel, and market reputation) before they are appointed, as well as on an ongoing basis to identify any potential integrity or reputational risks that may arise.

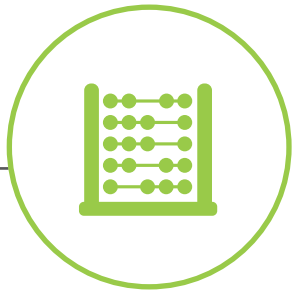
3 Is fraud risk management part of the overall enterprise risk management process?

Fraud risk management (FRM) is often considered as part of enterprise risk management programs. However, the objectives of a fraud risk management program are distinct and separate from those of an enterprise risk management program. Enterprise risk management programs focus on identifying financial risks (pricing, asset, liquidity, currency related risks), operational risks (customer satisfaction, product failure), strategic risks (competition, social trends, capital availability) and hazard risks (liability, damage due to natural calamities) [1]. Fraud risk management programs, in contrast, focus on issues pertaining to fraud, misconduct, noncompliance, and malpractice across all areas of business.

The Deloitte-BCCI whitepaper titled *Demystifying Fraud Risk Management for the Board*, released in March 2015, recommends that FRM should be run as an independent program to achieve better outcomes.

1 Source: https://books.google.co.in/books?id=qSYPBwAAQBAJ&pg=PA7&lpg=PA7&dq=%22Overview+of+Enterprise+Risk+Management%22+%28PDF%29.+Casualty+Actuarial+Society.+pp.+9%E2%80%9310.+Retrieved+2008-09-15&source=bl&ots=iwFY1vpE7t&sig=U4KISSsGX--cRNxV4jyyKbQA0As&hl=en&sa=X&ei=TpVtVdmeOIjY8gXIz4LACQ&ved=0CCcQ6AEwAg#v=onepage&q&f=falsety.+pp.+9%E2%80%9310.+Retrieved+2008-09-15&source=bl&ots=iwFY1vpE7t&sig=U4KISSsGX--cRNxV4jyyKbQA0As&hl=en&sa=X&ei=TpVtVdmeOIjY8gXIz4LACQ&ved=0CCcQ6AEwAg#v=onepage&q&f=false

Developing a Fraud Risk Assessment framework



4 Is there any framework recommended for developing fraud risk assessment? What should be the key elements of such an assessment?

The Companies Act, 2013, does not prescribe a framework or guidance for undertaking fraud risk assessment. However, the RBI has prescribed guidelines on fraud risk management to banks and the Institute of Chartered Accountants of India has released a guidance document focused on sensitizing internal auditors to detect fraud.

We have observed that several leading companies are adopting the Committee of Sponsoring Organizations of the Treadway Commission 2013 – Internal Control Integrated Framework (Revised COSO 2013 Framework) to develop their own fraud risk assessment framework. The key elements of a fraud risk assessment framework include:

- Identifying fraud schemes and conducting scenario based assessment on them to understand the most severe and the least severe fraud risks;
- Identifying circumstances that may present opportunities for fraud;
- Management override of controls and the impact on fraud;
- Potential fraud risks emerging from third parties/ outsourced service providers doing business for and on behalf of the company.

The Deloitte Forensic Point of View document titled *Building effective internal controls for better fraud risk management* describes fraud risk assessment in detail.

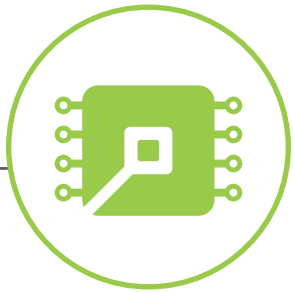
5 Who should be responsible for conducting fraud risk assessment? What skills should such individuals/ teams develop?

The responsibility for conducting fraud risk assessment usually lies with the fraud risk management team. While many organizations assign this responsibility to their internal audit team, some leading organizations appoint a separate fraud risk management team comprising of members from internal audit, management assurance, legal, risk and compliance, and IT security. The fraud risk management team, besides undertaking the fraud risk assessment, also performs continuous monitoring, review of high risk areas, and may also conduct or oversee fraud investigations.

To successfully undertake these activities, fraud risk management teams require deep understanding of how and why fraud is perpetrated, components of a fraudulent act, different types of fraud schemes and the impact of fraud on organizations. Therefore, the fraud risk management team needs to equip itself with technology and key investigation competencies, such as investigative interviewing skills, using data analytics to detect red flags, market intelligence gathering skills and evidence handling skills including use of forensic technology.

Leading organizations often appoint a fraud risk management champion (ideally an executive-level member designated as the chief risk officer or chief compliance officer) whose role would be to ensure that the objectives of the anti-fraud program are being met. Further, he/she would also oversee critical initiatives by translating policy level statements into simple action items to gain employee commitment. He/she is expected to periodically appraise the Board of directors about the effectiveness of fraud risk management processes and controls.

Using technology in fraud detection



6 Can you give some practical examples where data analytics could be successful in fraud detection? Does one need any specific tools for fraud detection and analysis?

At least 11 types of frauds can be detected through the use of data analytics on transactions, according to the Deloitte India Fraud Survey, released in 2014. They include theft of inventory, supply chain fraud, money laundering, mergers and acquisition fraud, financial misstatement, ecommerce fraud, cybercrime, counterfeiting, insider trading, bribery and corruption, and asset misappropriation.

Data Analytics tools analyze daily transactions and activities, such as purchasing, accounts payable, sales, inventory movements, employee shift records, etc. and identify anomalies or unusual patterns/ trends in the data that might be indicative of potential fraudulent activity.
This in turn can help develop appropriate priorities for case management and investigation.

Data analytics tools can be purchased off-the shelf or developed in house. Deloitte, for instance, uses its proprietary tool 'D-Tect' to integrate data across the business, basis which electronic data analysis is conducted and specific fraud risk management issues are investigated.

For organizations in the nascent stages of using data analytics, the Deloitte India Fraud Survey, released in 2014, recommends aligning specific IT controls with fraud risk management processes to possibly improve detection of fraud. Some measures include:

- Logging and maintaining an audit trail of activities
- Automated notifications (emails/ text messages) in cases of process overrides
- Active Threat Monitoring and Management
- Audio Visual monitoring
- Data Leakage Prevention (DLP) software
- Adequate control on devices (employee owned and office owned) containing confidential office data

Exploring Ethical Audits

7 What is an Ethical Audit? Is it part of the financial audits undertaken regularly or is it different?

Ethical audits are a possible means of assessing an organization's culture in terms of its employees' understanding of the code of business conduct/ ethics policy and analyzing employees' perceptions, attitude and their ability to identify specific fraud vulnerabilities. Ethical audits are not a part of financial audits routinely undertaken by organizations through departments such as risk and compliance, statutory audit etc.

Some of the ways in which ethical audits can be conducted include:

a. Employee survey on organizational culture
b. Employee ethics and fraud awareness survey
c. Fraud awareness training program
d. Ethical dilemma workshops
e. Fraud Vulnerability Workshops

8 Are there any guidelines to conduct Ethical Audits?

There are no specific guidelines prescribed for undertaking ethical audits under the Companies Act, 2013. However, in our experience, culture, including ethical behavior, can be a good benchmark for measuring an organization's susceptibility to fraud.

Understanding an organization's culture can help design effective antifraud controls. Therefore, we observe that several leading organizations have started undertaking ethical audits periodically (at least once, every two years) to evaluate employees' ethical quotient, the willingness to comply with the code of conduct, and identify and report emerging concerns. These ethical audits are customized by the organization based on their requirements, nature of operations, the larger industry practices, and size of operations.

Assessing effectiveness of a fraud risk management program

9 What are the visible indicators of success in a company's efforts to establish a fraud risk management program?

Companies that invest in building a fraud risk management program are able to build and demonstrate strong ethical culture within the organization and robust anti-fraud controls. Due to the presence of antifraud controls, such organizations are also able to detect and respond to incidents of fraud much more quickly and limit losses due to fraud, compared to organizations that lack anti-fraud controls [2].

10 How can one assess the effectiveness of the internal investigation process, as well as fraud awareness training programs?

The effectiveness of the internal investigation process can be assessed by observing how the organization manages to address employee and third party concerns on fraud, malpractice and misconduct reported using whistleblowing channels. Our observation is that organizations that demonstrate prompt and competent investigation and resolution of reported incidents are able to sustain confidence and trust amongst employees and stakeholders of its commitment to tackle fraud.

For employees to access whistleblowing channels, they would need to be aware of the fraud vulnerabilities in their respective areas of work, scenarios that qualify as fraud or violation of the code of conduct, and the presence of safe and confidential reporting channels within the company. Such sensitization is possible only when organizations have robust ongoing fraud awareness training programs for employees.

2 Source: The ACFE report to the Nations on Occupational Fraud and Abuse, 2014

Contact Us

Deloitte Touche Tohmatsu India Private Limited's Forensic practice provides fraud risk management services to leading organizations across all sectors and industries. We can help organizations diagnose their vulnerability to fraud, detect gaps in anti-fraud controls, recommend mitigating anti-fraud controls, continuous monitoring of systems, develop a fraud response plan, and investigate alleged cases of fraud.

For more details, please reach out to the below mentioned people.

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

Amit Bansal
Senior Director
Forensic
Tel: +91 22 6185 6764
Email: amitbansal@deloitte.com

Sumit Makhija
Senior Director
Forensic
Tel: +91 124 679 2016
Email: sumitmakhija@deloitte.com

Nikhil Bedi
Senior Director
Forensic
Tel: +91 22 6185 5130
Email: nikhilbedi@deloitte.com

KV Karthik
Senior Director
Forensic
Tel: +91 22 6185 5212
Email: kvkarthik@deloitte.com

Jayant Saran
Senior Director
Forensic
Tel: + 91 124 679 3607
Email: jsaran@deloitte.com

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


RISK

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. Deloitte Touche Tohmatsu India Private Limited ("DTTIPL" or "Deloitte India") is a member firm of Deloitte Touche Tohmatsu Limited.

This document and the information contained herein prepared by DTTIPL 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, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this document, 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.

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.

This document does not constitute an audit or a limited review performed in accordance with generally accepted auditing standards in India, or a due diligence or an examination of internal controls, or other attestation or review services or services to perform agreed upon procedures in accordance with standards established by the Institute of Chartered Accountants of India nor do they or will they constitute an examination of a forecast in accordance with established professional standards.

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.

Forensic and/or ethical audit does not constitute an audit or a limited review performed in accordance with generally accepted auditing standards in India, or a due diligence or an examination of internal controls, or other attestation or reviews or agreed upon procedures performed in accordance with standards established by the Institute of Chartered Accountants of India nor do they constitute an examination of a forecast in accordance with established professional standards.

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.