Fraud Risk Management and Corporate Governance in India

Suveer Khanna
Partner, Forensic Services
KPMG India Ltd.

Sanya Arora
Associate Director, Forensic Services
KPMG India Ltd.

Fraud occurrences are snowballing in India, with the diversity of fraud threats contributing to the alarming surge in the frequency of incidents. The range of frauds is widening with the cyber dimension, newly emerging risks of data theft and manipulation in addition to the existing risks of financial frauds by employees, vendors and other third parties. Effective Fraud Risk Management ('FRM') is one of the key pre-requisites for good corporate governance regardless of the nature and size of the organizations.

Association of Certified Fraud Examiners ('ACFE') released their 12th edition on "Occupational Fraud 2022: A Report to the Nations"[i] which covered about 133 countries across the world studying 2,110 cases. The research showed that about 7% (138 cases) emanated from South Asia. The study also revealed that:

a. Corruption accounted for the majority of fraud cases in this region (71%);
b. Managerial-level fraudsters made up 42% of the cases, followed by 28% and 27% by employee level and owner/executive-level fraudsters respectively.

As fraud risks become more prevalent and complex, FRM becomes more essential than ever, for companies to prevent financial losses, safeguard their reputation and brand, enhance employee morale and trust and boost investors' confidence.

The primary goal of a FRM framework is to proactively prevent fraudulent activities from taking place and put in place a system of alert generation for early detection in the event of occurrence of a fraud. A comprehensive FRM entails a systematic evaluation, detection and prevention strategy in an organization. By implementing established systems and processes, companies can effectively thwart fraud risks from both internal and external sources, identify their susceptibilities, and take appropriate measures such as augmenting their internal controls to ward off potential fraud schemes in the entire range of corporate functions, be it procurement, finance and accounts, IT, HR etc.

Regulatory perspectives on Fraud Risk Management

In response to the rapid technological advancements and the ever-growing high-profile scandals, Indian regulators such as the Securities and Exchange Board of India (SEBI), Reserve Bank of India (RBI), and Ministry of Corporate Affairs (MCA) have recognized the urgent need to mandate the companies to have a strong and robust FRM framework.

Some of the key regulatory requirements that Indian companies must comply with are:

I. Regulations stipulated by The Companies Act, 2013

To combat the rising number of corporate frauds in India, key amendments were brought in The Companies Act 2013, which amplifies the focus on implementing a robust FRM framework. The key changes to highlight are:

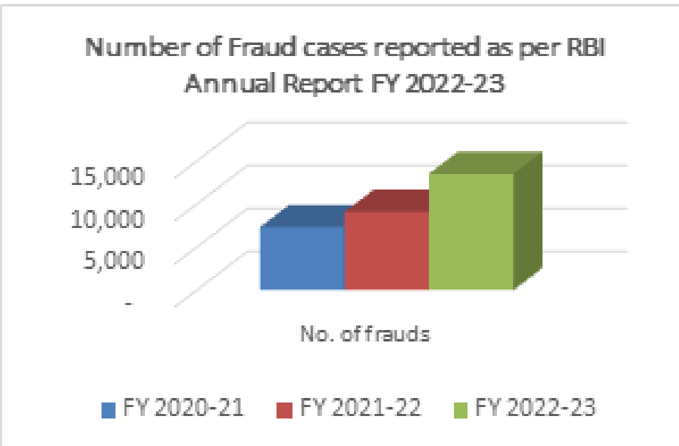
a. The 'Directors Responsibility' statement shall include a statement indicating development and implementation of a Risk Management policy including identification of elements of risks, which in the opinion of the Board may threaten the existence of the company.
b. Audit committee including the independent directors of companies must satisfy themselves on the integrity of financial information, and that the financial controls and the systems of risk management are robust and defensible.
c. As per Section 210 (1) of the Act[ii], the Central Government is at discretion to order Serious Fraud Investigation Office ('SFIO')[iii] an investigation into the affairs of a Company- (a) on the receipt of the registrar or inspector, (b) on intimation of a special resolution passed by a company that the affairs ought to be investigated, (c) in public interest.

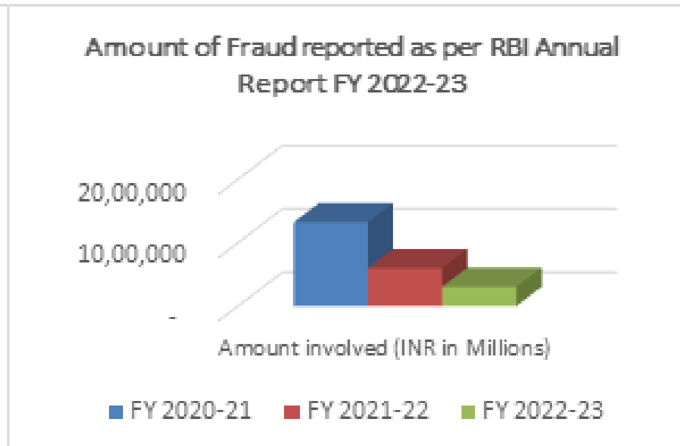
As per a recent Circular[iv] dated 26 June 2023 issued by National Financial Reporting Authority ('NFRA'), auditors are obligated to report to the Central Government and the Board/Audit Committee, if they have observed any suspicious transactions that indicate reasons to believe that an offence of fraud is being or has been committed against the company by its officers or employees. Resignation from an audit engagement does not absolve auditors of their reporting obligations or the consequences of non-reporting of fraud.

II. Regulations stipulated by Reserve Bank of India (RBI)

The annual reports published by the RBI have drawn attention to a rise in the number of fraud cases reported by the banks over the past three fiscal years. The study suggests that although the RBI's annual report shows a decrease in the reported amount of fraud over the last three years, there has been a significant 48% increase in volume compared to the fiscal year 21-22.

It further indicates that while private sector banks reported maximum number of frauds, public sector banks continued to contribute maximum to the fraud amount during FY 2022-23. Below table summarises the total fraud cases and amount of fraud across the entire banking sector over the last three financial years:





RBI has issued several master directions[v] and circulars on monitoring and reporting frauds in NBFCs and commercial banks. These directions provide a framework enabling the organizations to detect and report fraud at early stages and take timely actions.

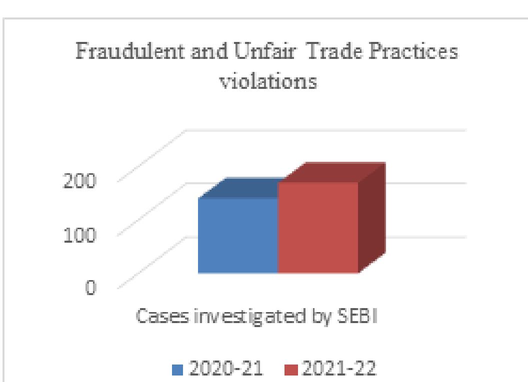
Banks and NBFCs governed by RBI regulations are required to align their FRM policy in line with the Master Direction. Further, these organizations are mandated to report such frauds to their Board and to RBI on a regular basis based on the threshold limits set in the Direction. Additionally, as per the above stated Master Directions, banks/NBFCs are also required to set up a special committee to monitor all cases of fraud involving amounts of INR 10 million and above. With the due approval of the board, they are directed to frame internal policy for FRM and fraud investigation function, based on the governance standards relating to the ownership of the function and accountability.

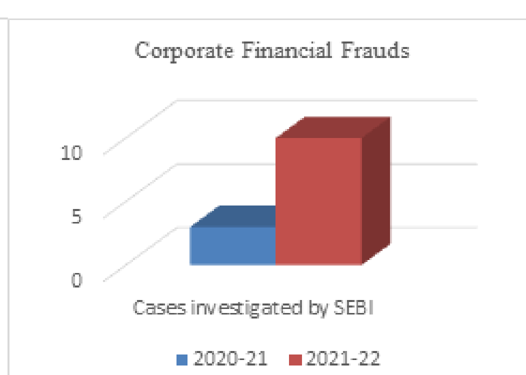
A good Corporate Governance serves as a very important factor in control of fraudulent activities. The RBI has unambiguously stated that senior management must prioritize the roles of fraud risk management, fraud monitoring, and fraud investigation functions. A perspective of RBI's vision for tackling risks emanating from frauds are:

a. Streamlining the process of data collection from all the banks and adoption of risk-based model developed for KYC/AML supervision;
b. Improving efficacy of Early Warning Signal (EWS) framework, strengthening fraud governance and response system, augmenting data analysis for monitoring transactions and dedicated market intelligence unit;
c. A pro-active cyber immunity surveillance framework to automate data flow from banks to RBI for better analysis;
d. Continuous study of large value frauds with the involvement of banks/NBFCs and suggest measures for early detection and timely mitigation of risks arising out of fraud.

III. Regulations stipulated by Securities and Exchanges Board of India (SEBI)

SEBI's Corporate Finance Investigation department conducts comprehensive investigations into violations of laws and regulations, including financial reporting requirements. As per SEBI's Annual report 2021-22, the cases investigated by SEBI, involving market manipulation and price rigging, insider trading and others under Fraudulent and Unfair Trade Practices violation and corporate financial investigations are as follows:





In compliance with SEBI LODR (Listing Obligations and Disclosure Requirements) regulation 27[vi], the top 1000 listed entities must include confirmation of their adherence to the risk management committee requirements in their quarterly compliance report on Corporate Governance. The reporting requirements necessitate the inclusion of information regarding any cyber security incidents, loss of data or documents in the quarterly compliance report. The entities are required to formulate detailed risk management policy which shall include:

a. Measures for risk mitigation
b. Business continuity plan
c. Framework for identification of internal and external risks faced by such entities, including financial, operational, environmental and cybersecurity among other risks.

The **Whistleblowers Protection Act 2014** requires all SEBI listed companies to implement a whistleblower policy in order to augment transparency and accountability, incentivize employees who report concerns, safeguard them against reprisals and combat insider trading.

IV. Regulations stipulated by Insurance Regulatory and Development Authority (IRDA)

According to India forensic research dated September 12, 2022, the insurance sector in India loses approx. INR 30,000 crores every year due to fraud. In other words, every insurer loses 8.5% of its revenue to frauds. Nearly 70 per cent of these frauds are committed through false documents. There was also an overall increase in insurance fraud investigations after the onset of Covid-19, with 55% of respondents confirming that their professional activities related to fraud-fighting have either increased overall or increased under a specific area of operation during the pandemic.

In the wake of rising frauds in the Insurance sector, the Insurance regulator, IRDAI is now considering a recommendation to set up an independent investigation agency similar to SFIO. This decision was made to establish an independent authority to investigate, prevent, adjudicate, and penalize companies that breach regulatory requirements.

As per the IRDAI Fraud Monitoring Framework[vii] dated January 21st 2013, the IRDAI classified frauds in the insurance sector under three heads -- claim fraud or policyholder fraud, intermediary fraud and internal fraud.

As per the above regulations, every Insurance company is mandated to have the Fraud Monitoring Function as a separate vertical that shall ensure effective implementation of the anti-fraud policies. They shall be responsible for laying down procedures for internal reporting from/and to various departments, to educate employees, intermediaries and policyholders on identification and prevention of frauds. Further, they must regularly update regulatory authorities on such incidents as well as steps taken to contain such scenarios within a stipulated time.

The Insurance company's Board of Directors are also mandated by the IRDA to review their respective Anti-Fraud policies on an annual basis, and at such other intervals as may be considered necessary. Further, as per the Guidelines for Corporate Governance for Insurers in India, 2016[viii] issued by IRDAI:

a. Insurers shall set up a separate Risk Management Committee to implement the company's Risk Management Strategy.
b. Formulation of a Fraud monitoring policy and framework for approval by the Board.
c. Monitor implementation of Anti-fraud policy for effective deterrence, prevention, detection, and mitigation of frauds.
d. The Board or the Risk Management Committee should be periodically apprised about the outsourcing arrangements entered by the insurer and also confirmation to the effect that they comply with the stipulations of the Authority as well as the internal policy be placed before them.

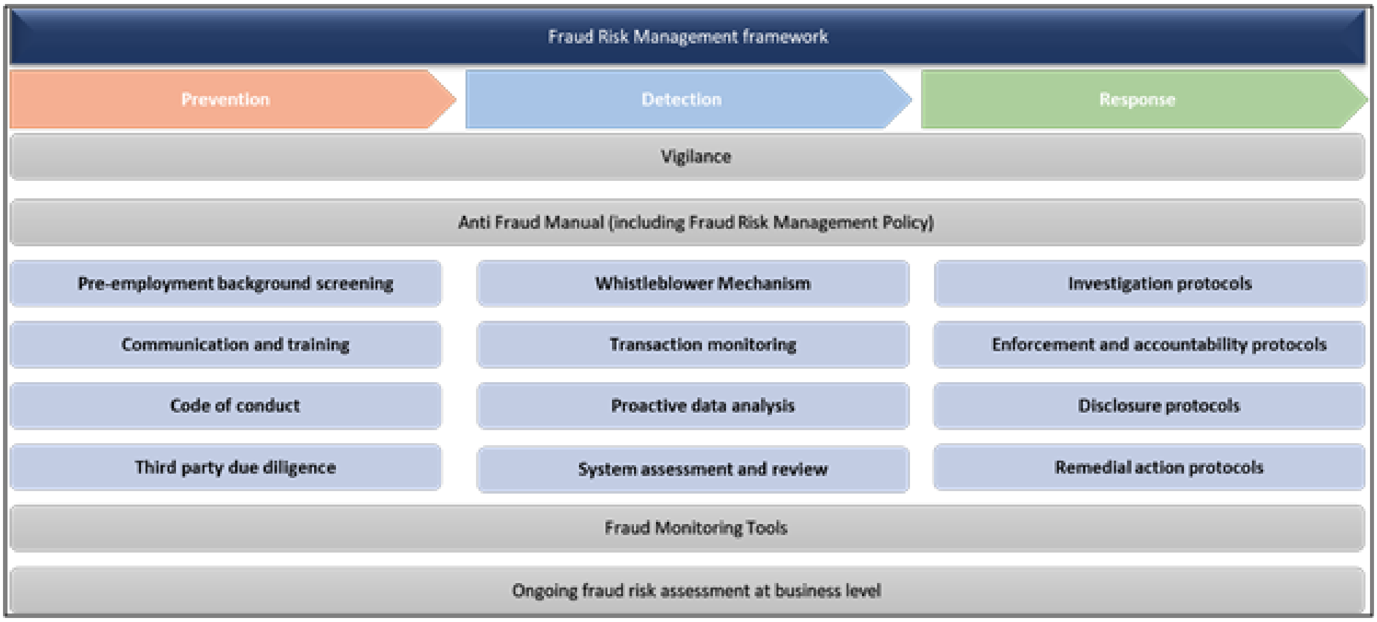
V. Corporate Liability under Prevention of Corruption Act, 1988 and Prevention of Corruption (Amendment) Act 2018

Prevention of Corruption Act ('POCA'), 1988: In 2018, the Government of India amended the Prevention of Corruption Act (POCA), with the aim of making both the bribe givers and takers accountable under the law. A provision creating liability for corporates and other business entities to put in place a framework for preventing corruption was introduced to address supply side of corruption. This amendment marks a significant change in the approach towards tackling corruption in the country. However, POCA provides immunity to organizations that can demonstrate a valid defense mechanism to prove that it had adequate controls in place. Therefore, it is crucial for companies to establish an efficient compliance framework that enables them to undertake timely risk assessments, conduct due diligence on employees and vendors, and regularly monitor and evaluate the adequacy of their internal controls.

An Ideal Fraud Risk Management framework

An effective FRM framework is critical for preventing and detecting frauds by identifying potential risks, taking preventive measures, deploying monitoring and detection protocols and providing response guidelines. Implementing a well-functioning FRM framework can not only help companies to avoid regulatory penalties but also helps to significantly mitigate the risks of fraud and promotes a more secure and reliable business environment. An effective FRM framework is heavily reliant on technology to provide an array of tools and solutions that can automate the prevention and detection of fraud risks, to a large extent.

Outlined below is an example of an optimal FRM framework that can be executed to establish effective anti-fraud controls:



Here is a list of best practices that companies may follow to ensure the successful implementation of an effective FRM framework:

a. Conduct periodic fraud risk assessment and dipstick reviews to identify and address any gaps in the existing controls that could be exploited;
b. Segregation of duties to ensure adequate checks and balances are in place and each transaction is reviewed by different parties, reducing the risk of fraud;
c. Sectoral fraud themes should be regularly analyzed and necessary preventive controls have to be incorporated in the framework;
d. Proactive data analytics using tools with built in algorithms and machine learning capabilities to identify anomalies, patterns and deviations in financial and operational data;
e. Surprise audits based on the red flags from data analytics;
f. Dedicated Ethics or risk compliance team to oversee and monitor effectiveness of key controls, while also conducting investigations in response to the complaints or red flags and for ensuring third party/employee due diligence, compliance awareness and trainings etc.;
g. Regular training to employees to emphasize the significance of fraud prevention and detection, as well as to raise awareness about their rights and protections under the whistleblower policy;
h. “Defining formal measures to mitigate misconduct may include implementing policies such as whistleblower protection, escalation procedures, and effective compensation schemes, among others;
i. Promote culture of preventive vigilance, to identify the cases of misconduct/frauds such at an early stage.

---

[i] legacy.acfe.com/report-to-the-nations/2022/
[ii] Chapter XIV Inspection, Inquiry, and Investigations Section 210 (1) of The Companies Act, 2013
[iii] SFIO is an organization set up under the MCA for investigation and prosecution of white-collar crimes and to uncover corporate fraud.
[iv] Circular No. NF-25013/2/2023
[v] RBI/DBS/2016-17/28 Master Directions on Frauds – Classification and Reporting by Commercial banks and select FIs and RBI/DNBS/2016-17/49 Monitoring of Frauds in NBFCs
[vi] SEBI/LAD-NRO/GN/2021/22
[vii] IRDA/SDD/MISC /CIR/009/01/2013
[viii] IRDA/F&A/GDL/CG/100/05/2016