MOORE Singhi

Building Resilience to Fraud

Fraud costs billions of dollars in damage to companies, governments, and individuals each year. An understanding of types of frauds and triggers will hep build a strong fraud mitigation strategy.

A. Types of Frauds:

The fraud universe can be categorised into three buckets.

Fraudulent Statements	Asset Misappropriation	Corruption
• Financial	• Cash	• Conflict of interest
• Non-Financial	• Non-Cash	• Bribery & Extortion

1. Financial frauds:

Financial statement fraud occurs when a company alters its financial statements to make it appear more profitable than it is. Financial statement fraud is the least common type of fraud but the costliest. Typical frauds include:

- Overstating revenues by recording future expected sales.
- Inflating an asset's net worth by applying the incorrect depreciation schedule.
- Hiding obligations and/or liabilities from a company's balance sheet.
- Incorrectly disclosing related-party transactions and structured finance deals.
- Understate revenues in one accounting period and maintain them as a reserve for future periods with worse performances, also known as cookie-jar accounting.

2. Asset Misappropriation:

Common techniques and Schemes Used in Asset Misappropriation include:

Embezzlement: Embezzlement is typically carried out by employees who have access to the company's finances. These individuals exploit their position and knowledge of the internal control systems to divert funds for personal use. Regular audits and strong internal controls are essential for prevention.

Fake Vendors and Shell Companies: Employees and external parties collude to create fake vendors and shell companies. Thereafter, they generate fake invoices for non-existent goods or services, approve the fake invoices and divert company funds to the shell companies. Implementing strong vendor vetting processes invoice and payment verification procedures are essential to prevent this type of fraud.

Check and Payment Tampering: Check and payment tampering techniques might include changing payee names, altering check amounts, or intercepting and altering electronic payment instructions. Employees responsible for payment processing are often the perpetrators, exploiting their position to bypass controls. Secure payment methods, segregating duties, and regular reconciliation of accounts can mitigate these risks.

Skimming and Cash Larceny: Both involve cash theft. Skimming occurs when an employee takes cash before it's recorded in accounting records, such as stealing part of the cash sales before depositing the rest. Cash larceny is stealing cash after it has been recorded; for instance, taking money from the cash register after the sales have been logged. Both methods require the perpetrator to manipulate records to cover up the theft, making reconciliation and regular audits vital for detection.

Inventory Theft and Fraud: This type of fraud scheme refers to the physical theft of inventory and manipulating records to cover up the theft or inflate the value of inventory. This might include falsifying receiving reports, altering shipping documents, or tampering with physical counts. Implementing stringent inventory control measures, employing surveillance systems, and conducting unannounced inventory counts can help uncover and prevent these schemes.

3. Corruption:

A conflict-of-interest fraud occurs when an employee has an undisclosed personal interest in a transaction.

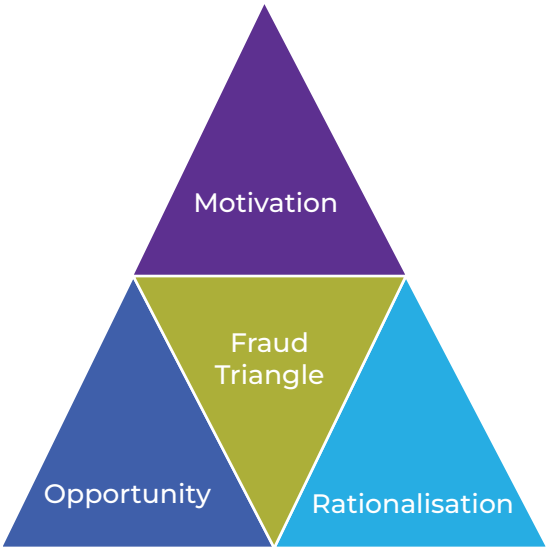
Bribery examples include paying procurement staff to sway their decision in favour of the paying company, giving an expensive gift to a bank manager to secure a loan, and various forms of kickbacks.

B. Why Frauds Occur–The Fraud Triangle

Motivation: Motivation is typically based on either greed or need. Many people are faced with the opportunity to commit fraud, and only a minority of the greedy and needy do so. Personality and temperament, including how frightened people are about the consequences of taking risks, play a role.

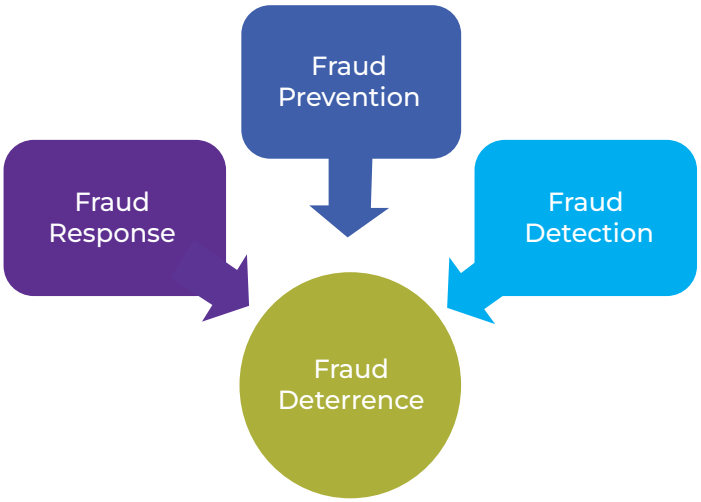
Opportunity: In terms of opportunity, fraud is more likely in companies where there is a weak internal control system, poor security over company property, little fear of exposure and likelihood of detection, or unclear policies about acceptable behaviour. Some employees are totally honest, some are totally dishonest, but many are swayed by opportunity.

Rationalisation: Many people obey the law because they believe in it and/or are afraid of caught. However, some people may be able to rationalise fraudulent actions as necessary, harmless, or justified.



C. Fraud Mitigation Strategy

The most effective way to mitigate fraud is to adopt methods that will decrease motive, restrict opportunity, and limit the ability for potential fraudsters to rationalise their actions.



3. Prevention:

Prevention techniques include the introduction of policies, procedures and controls, and activities such as training and fraud awareness to stop fraud from occurring.

A. Internal controls:

A strong system of internal controls is the most valuable fraud prevention device by a wide margin. Having sound internal control systems is also a requirement under the Companies Act, IFC and various corporate governance codes. Internal controls include:

1. Segregation of duties
2. Authorisation
3. Retention of records
4. Account reconciliations
5. Supervising operations
6. Physical safeguards (CCTV/Locks/barriers)
7. Top level reviews
8. IT general controls
9. IT application controls

B. Strong ethical culture:

Ethical behaviour needs to be embedded within the culture of an organisation. Commitment from senior management and 'tone at the top' is key. Employees are more likely to do what they see their superiors doing than follow an ethics policy. An ethics framework would include:

1. Code of business ethics
2. Statement of ethical values
3. Training on ethical standards
4. Hotline
5. Helpline for advice on ethics at work
6. Incentives for staff to uphold ethics

2. Detection:

A fraud detection strategy should involve use of analytical and other procedures, and audits to highlight anomalies, and the introduction of reporting mechanisms that provide for communication of suspected fraudulent acts.

1. Whistle blowing hotline
2. Internal tip off
3. By accident
4. External tip off
5. Law enforcement investigation
6. Change of personnel duties
7. Internal audit
8. External audit
9. Corporate security
10. Risk management

3. Deterrence:

Fraud detection acts as a deterrent by sending a message to likely fraudsters that the organisation is actively fighting fraud and that procedures are in place to identify any illegal activity that has occurred. The possibility of being caught will often persuade a potential perpetrator not to commit a fraud.

4. Response:

A consistent and comprehensive response to suspected and detected incidents of fraud is important. This sends a message that fraud is taken seriously, and that action will be taken against perpetrators. Each case that is detected and investigated should reinforce this deterrent and, therefore, act as a form of fraud prevention. A response framework should include:

1. Reporting
2. Investigation
3. Disciplining the individual
4. Recovery of stolen property
5. Enhancing controls

Conclusion

A sound ethical culture and an effective system of internal control are essential elements of an anti-fraud strategy. Effective internal controls reduce exposure to financial risks and contribute to the safeguarding of assets, including the prevention and detection of fraud.

Mazyar Kotwal
Senior Partner – Risk Advisory Services

services@moore-singhi.in
Offices : Kolkata I Delhi NCR I Mumbai I Chennai I Bangalore I Raipur