SECTION - D

FORENSIC AUDIT AND ANTI-MONEY LAUNDERING

Forensic Audit 17

This Module includes:

Forensic Audit

SLOB Mapped against the Module

To develop detail understanding of the financial forensics and forensic audit techniques to identify the scope left for committing frauds and recommend appropriate corrective actions. (CMLO 2a, b)

Module Learning Objectives:

The primary objective of this Forensic Auditing and Accounting is to empower the investigator or the overseer with the fundamentals of accounting practices and financial statement analysis. In-depth study of the procedures of fraud detection including methodologies to identify and categorize fraudulent practices. After studying this module, the students will be able to –

- Identify cases of fraud
- Prevent and reduce cases of fraud through the implementation of recommendations and advice, through internal control in the company
- Participate in the design and creation of fraud prevention programs
- Evaluate Internal Control Systems for adequacy to prevent formula and unethical activities.
- Perform investigation and collection of evidence that will be placed in the hands of the judicial authority.

Introduction

17

A forensic audit is an evaluation and examination of an individual's or a firm's financial records to stem up evidence that can be used in a legal proceeding or court of law. Forensic auditing is a specialization within the accounting field, and most large accounting firms have a forensic auditing department. Forensic audits necessitate auditing and accounting procedures as well as expert knowledge about the legal outline of such an audit.

Generally, Forensic audits cover a wide range of investigative activities. A forensic audit may be directed to prosecute a party for embezzlement, fraud, or additional financial crimes. Moreover, the auditor may also be called to help as an expert witness during trial proceedings of a forensic audit. Forensic audits could also involve situations such as disputes related to business closures, bankruptcy filings, and divorces that do not involve financial fraud.

Forensic audit investigations may interpret, or confirm, numerous kinds of illegal activities. In general, a forensic audit is used if there is a possibility that the evidence collected would be used in court in its place of a normal audit.

The forensic audit process is similar to a traditional financial audit accepting investigation, planning, assembling evidence, and writing a report with the added steps of a potential appearance in court. The lawyers offer evidence that the crime is one or the other discovered or disproved, which agrees with the harm sustained. In this procedure, they will explain their conclusions to the respondent should the case go to trial in front of the judge.

The reasons are as follows:

Common Areas of Forensic Audit:

The Forensic Auditor may be asked to investigate many different areas of fraud.

It is useful to categorise these investigations into following groups to provide an overview of the wide range of investigations that could be carried out.

The 3 category of frauds are corruption, asset misappropriation, and financial statement of fraud.

1. Curruption

There are 3 types of corruption fraud.

a) Conflict of Interest

In a conflict of Interest fraud, the fraudster exerts their influence to achieve a personal gain which detrimentally affects the company.

The fraudster mat not benefit financially, but rather receives an undisclosed benefit as a result of the situation.

For example, a manager may approve the expenses of an employee who is also a personal friend in order to maintain that friendship. Even if the expenses are inaccurate.

b) Bribery is when money (or something else of value) is offered in order to influence a situation.

c) Extortion is the opposite of bribary, and happens when money is demanded (rather than offered) in order to secure a particular outcome.

2. Asset Misappropriation

By far the most common frauds are those involving asset misappropriation, and there are many different types of fraud which fall into this category.

The common feature is the theft of cash or other assets from the company.

For example :

Cash Theft

The stealing of physical cash, for example petty cash, from the premises of the company

Fraudulent disbursements

Company funds being used to make fraudulent payments.

Common examples include billing frauds, where payments are made to fictitious supplier, and payroll frauds, where payment are made to fictitious employees (often known as ghost employees)

Inventory Frauds – the theft of inventory from the company

Misuse of Assets – employees using company assets for their own personal interest

3. Financial Statement Fraud

It is also known as fraudulent financial reporting.

It is a type of fraud that causes a material misstatement in the financial statements.

It can include deliberate falsification of financial statements which shall include omissions of :

Transactions, balances or disclosures

From the financial statements or

The misapplication of financial reporting standards.

This is often carried out with the intention of presenting the financial statements with a particular bias, for example concealing liabilities in order to improve any analysis of liquidity and gearing.

Introduction to Forensic Audit

17.1

A forensic audit is an analysis and review of the financial records of a company or person to extract facts, which can be used in a court of law. Forensic auditing is a specialty in the accounting industry, and most major accounting firms have a department of forensic auditing. Forensic audits include experience in accounting and auditing practices as well as expert knowledge of forensic audit's legal framework.

Forensic audits cover a large spectrum of investigative activities. There may be a forensic audit to prosecute a party for fraud, embezzlement, or other financial crimes.

The auditor may be called in during the process of a forensic audit to serve as an expert witness during trial proceedings. Forensic audits could also include situations that do not involve financial fraud, such as bankruptcy filing disputes, closures of businesses, and divorces.

When it comes to auditing, many organisations consider it is as simply a statutory requirement for getting the financials examined by a certified accountant to ensure compliance. However, this type of audit (financial audit) is just one of many other types of audits that any organisation would undergo. A forensic audit is one among such audits which involve an examination of past financial records of an entity to detect any illegal action, manipulation in the books of accounts, siphoning of funds, etc. The forensic audit begins with the suspicion and doubts and ends with the performance of investigation procedures either to confirm the case or dispel the suspicion.

Unlike financial audits which are focused more on statutory compliance, forensic audits are designed to investigate the financial records of an entity to derive evidence support of fraud that can be used in a court of law or legal proceedings.

It is an independent, comprehensive, and scientific approach to reviewing an entity's financial statements. To determine its accuracy, free from material misstate, and evidence be used in a court of law or legal proceedings.

Reasons for Conducting a Forensic Audit:

Forensic audit investigations may expose, or confirm, various kinds of illegal activities. Normally, instead of a normal audit, a forensic audit is used if there is a possibility that the evidence gathered would be used in court.

The forensic audit process is similar to a traditional financial audit planning, gathering evidence, and writing a report with the additional step of a possible appearance in court. The lawyers on both sides offer evidence that the crime is either discovered or disproved, which decides the harm sustained. They explain their conclusions to the defendant should the case go to trial before the judge.

Investigation Methodology of Forensic Audit:

Forensic Audit can be done with the adoption of the procedure detailed below :

1. Accepting the Investigation

A forensic audit is assigned to an independent firm / group of investigators in order to conduct an unbiased and truthful audit investigation.

Thus, when such a firm receives an invitation to conduct an audit, their 1st step is to determine whether or not they have the necessary tools, skills and expertise to go forward with such an investigation.

They need to do an assessment of their own training and knowledge of fraud detection and legal framework.

Only when they are satisfied with such considerations, can they go ahead and accept the investigation.

2. Planning the Investigation

Planning the investigation is the key in a forensic audit.

The auditors must carefully ascertain the goal of the audit so being conducted and to carefully determine the procedure to achieve it, through the use of effective tools and techniques.

Before planning the investigation, they should be clear on the final categories of the report, which are as follows.

- Identifying the type of fraud that has been operating, how long it has been operating for, and how the fraud has been concealed
- Identifying the fraudsters involved
- Quantifying the financial loss suffered by the client
- Gathering evidence to be used in court proceedings
- Providing advise to prevent the recurrence of the fraud

Fraud Triangle and Fraud Risk

A fraud triangle is a tool used in forensic auditing that explains 3 inter related elements that assist the commission of fraud.

- Pressure (motive)

  Motivation or incentive to commit fraud
- Opportunity

  Ability to carry out misappropriations of cash or organisational assets
- Realisation

  Justification for dishonest actions

Planning also includes the identification of the best way / mode to gather evidence.

Thus, it is necessary that ample research is done regarding certain investigative , analytical, and technology-based techniques, and also related legal process, with regards to the outcome of such investigation.

3. Gathering Evidence

The investigators can use the following techniques to gather evidence.

1. Reviews of Public Documents and Conducting background Investigations / Checks

   The documents made available to public are scrutinised as they are easiest to obtain.

   Public documents would include any information in the public database, the corporate records, and any legally available information on the internet.

   Also, back ground checks of a particular company are done to see past dealings of the business

2. Conducting Detailed Interviews

   Conducting an interview is an essential technique that can transform an unwilling person into a source of valuable information.

   It helps in fully understanding all the facts.

   An interview should be conducted by accurately assessing the gravity of the situation and preparing the questions according to it.

   Discussion should take every detail into account and look at the greater picture to figure it out the magnitude of the illegal activity and the culprit responsible.

3. Gathering Information from Trustworthy Sources

   Information provided by a confidential and trustworthy source can be precious to any case.

   When a piece of information is gained from a confidential source or a confidential informant, all the necessary precautions should be taken to hide of the so-called cause.

   A forensic accountant should try to have as many confidential sources as possible because such sources can virtually guarantee a correct result.

4. Conducting Surveilance

   This can be done physically or electronically and is one of the conventional measures to uncover any fraud.

   It can be done by monitoring and tracking all the official emails and messages.

5. Going Undercover

   This is an extreme measure and should be used only as a last resort.

   It is best left to the professionals as they know how and where to conduct the investigations.

   Even a small mistake while being undercover can signal the offender that something is wrong and the person might vanish / disappear from the scene.

6. Analysing the Financial Statements

   This is a special tool for finding out the fraud committed.

   Analysis of these statements can help a forensic accountants figure out the scam.

7. Analysing The Evidence Gathered

   Proper analysis of the obtained evidence can point to the guilty party.

   It shall also assist in understanding the extent of the fraud committed in the business.

   Furthermore, this analysis would also help understand how secure the company is against financial scams and installing various austerity measures to prevent any such future situation.

4. Reporting

The reporting stage is the most obvious element in a forensic audit.

After investigating and gathering evidence, the investigating team is expected to give report of-

1. The findings of the investigation

2. Summery of evidences collected
3. Conclusion about the loss suffered to the fraud
4. How fraud was planned and how it unfolded
5. The whole trail of events and
6. Suggestions to prevent such fraud in future

5. Court Proceedings

Here, the auditors are called to jurisdictional court.

It is important that they lay down the facts and findings in an easily understandable and objective manner for every one to comprehend so that the desired action can be taken up.

They need to simplify the complex accounting processes and issues for others to understand the evidence and its implications.

Need for Forensic Audit:

As of now, forensic auditing has emerged as a specialized field in the industry that requires a specific skill set to detect the fraud, leaving no scope for overlap, but to determine an organisation's needs, forensic auditing is significant in dealing with early warning signals of fraud. Thus, there are a few instances on the occurrence of which an entity should direct for forensic audit like:

I. Theft of business information or where business systems have been hacked.

II. Issues identified by Whistle-Blowers.

III. Reconciliations resulted in unidentified material differences.

IV. Suspicious of fraud or illegal activity.

V. Turnover has occurred and balances are showing negative results.

Forensic Audit Procedures:

Since the forensic audit is more of an investigation and collection of evidence, it is of great importance that the audit should be conducted with an attitude of professional scepticism. However, a scientific approach involving the use of forensic audit procedures should be used to conduct the assignments. These procedures are more towards detecting possible material misstatements in the financial records that result in fraudulent activities. Besides, forensic data analysis and fraud investigation techniques, a tool named 'triangle' also are used for addressing the presence of three-element that are common to any fraud being committed:

- Incentives- a motive that drives a person to commit fraud.
- Attitude- an ability to rationalize fraudulent behaviour.
- Opportunity- that enables a person to commit fraud.

Investigation Methodology of Forensic Audit:

The forensic audit investigation is the utilization of specialized investigation skills to conduct the forensic audit engagements in such a manner that the outcome can be presented in a court of law as evidence. The auditor should use an approach considering both the aspects of whether the fraud could have occurred and whether the fraud could not have occurred. With this approach, the forensic auditors will be able to bring the reality closer to the general,

public especially the circumstances where perception and reality are not aligned. An auditor can follow a nine-step method for fact-finding in case of forensic audit engagements:

- Accept the forensic audit engagement.
- Evaluate the allegations or suspicions.
- Conduct due diligence background notes.
- Complete the preliminary stage of the investigation.
- Check the prediction assuming that there will be litigation.
- Begin with an external investigation.
- Gathering the required proofs and evidence.
- Preparing report on findings; and
- Court proceedings.

Common Areas of Forensic Audit:

With the increase in financial fraud popularly known as white-collar crime, forensic accounting and auditing has emerged as prominent to ensure the financial growth for businesses and the economies as well. Some of the common areas that are to be in elected for forensic audits are:

- Asset Misappropriation.
- Instances of Corruption.
- Extortion.
- Financial Statement Fraud.
- Conflict of interest.

Hence, forensic auditing is a detailed examination of past financial records which requires the expertise of professionals not only in accounting and auditing but also in the area of assessing legal framework and fact-finding. The forensic auditor is expected to adopt a practical approach to deal with the numerous loopholes which may arise during investigation procedures. With the key benefits of increased credibility, expert accounting, enhanced effectiveness, and accuracy, the forensic audit is seen as a rapidly growing area in the detection and prevention of fraud and white-collar criminal activities.

Business Frauds:

Corporate fraud consists of illegal or unethical and deceptive actions committed either by a company or an individual acting in their capacity as an employee of the company. Corporate fraud schemes are often extremely complicated and, therefore, difficult to identify. It often takes an office full of forensic accountants' months to unravel a corporate fraud scheme in its entirety.

When corporate fraud is perpetrated by the top executives of a large corporation, the fraud often extends to billions of dollars in scale. The victims of corporate fraud are consumers or clients, creditors, investors, other businesses, and eventually, the company that is the source of the fraud and its employees. When it is finally discovered, the company committing the fraud is often left in ruins and forced to declare bankruptcy.

- Corporate fraud consists of illegal, deceptive actions committed either by a company or an individual who is an employee of the company.
- Many corporate fraud schemes are highly complicated accounting schemes used to inflate a company's apparent profits and may take years to detect.
- When massive corporate fraud is eventually discovered, it can take down even huge multinational companies with billions in annual revenues.

Much of the money illegally obtained through corporate fraud is often never recovered, after being spent long ago by the perpetrators.

Why Do Corporate Frauds Happen?

(a) **The Desire or Perceived need to attract or Retain Investors:** Corporate fraud commonly occurs for the same reason as any other fraud scheme-greed. However, amid the highly competitive global business environment of the modern world, it may also occur for other reasons. Many corporate fraud schemes consist of fraudulent accounting schemes used to make a company appear more profitable than it is. The impetus behind such schemes is the desire or perceived need to attract or retain investors.

(b) **Problems or defects with a Company's Products:** Another cause of corporate fraud may be problems or defects with a company's products, which it tries to hide. Several recent corporate fraud cases have occurred with pharmaceutical companies that attempted to hide certain side effects or dangers associated with using certain medicines they manufactured and sold.

Government regulatory authorities, the Securities Exchange Board of India (SEBI) and the Securities and Exchange Commission (SEC) in the United States, use laws and regulations to try to prevent, detect and punish corporate frauds. However, fraud may go undetected for many years before it becomes apparent to authorities, especially if the guilty company is a private company that is not required to publicly disclose its financial records.

(c) **Major Corporate Fraud Cases in the World:** Due to the rise of so many large, multinational corporations and conglomerates, almost all of the largest corporate fraud cases have occurred within the past five decades. The following are some of the biggest incidences of corporate fraud on record:

(i) **Enron Company:** One of the most notorious cases of corporate fraud is the Enron scandal. At its height, Enron, a major energy company, was raking in billions upon billions in profits. However, when the company began to face declining revenues and debt troubles, company executives hid the facts through massive accounting fraud.

In the end, both Enron and its accounting firm, Arthur Andersen, went under. Thousands of employees lost their jobs, and Enron's creditors and investors lost billions.

The Enron Accounting scandal is credited with resulting in the passage of the Sarbanes-Oxley Act, which required more transparency in companies' financial reporting and imposed significantly harsher penalties on any company caught for committing accounting fraud.

(ii) **Waste Management:** Waste Management, the largest garbage and recyclables collector in the United States, appeared to be one of the most financially sound companies in the United States in the early 1990s. Investors eagerly bought up the company's stock, driving its price steadily higher.

However, when a New Chief Executive Officer (CEO) assumed the post in 1998, he eventually discovered that, like Enron, Waste Management previously perpetrated a multi-billion-dollar accounting fraud in an attempt to pump up its profitability numbers.

Unlike Enron, Waste Management was able, under its new leadership, to survive the resulting scandal, penalties from the Securities and Exchange Commission (SEC), USA, and a multi-million-dollar lawsuit by investors.

(iii) **ZZZZ Best Company:** The story of ZZZZ Best, a carpet cleaning company founded by a 15-year-old, is a rags-to-riches-to-rags story. Within six years of the company's founding, its entrepreneur owner was able to take the company public, with a valuation of approximately $300 million. There was just one problem- Barry Minkow, the founder, and owner of ZZZZ Best had made up out of thin air practically all of the company's alleged "Customers".

Minkow was keeping the company afloat by using money acquired from new investors to pay off previous investors. In short, engaging in a classic Ponzi scheme. Before Minkow could generate enough business to cover his fraud tracks and hopefully right the company's finances, his fraud scheme was discovered.

The result was that ZZZZ Best, once an inspiring success story, went completely burst just a few months after the Company's initial public offering (IPO).

(iv) **Wirecard Company:** One of the more recent corporate fraud cases is that of Wirecard, a payment transfer and processing company in Germany. In early 2020, accounting auditors discovered a whopping $2 billion discrepancy between the company's books and the actual money it held.

Like many corporate fraud schemes, Wirecard's cooking of its books had been going on for several years before it was detected. Wirecard was forced to declare bankruptcy, and its CEO was arrested by German authorities.

(v) **Wells Fargo & Company:** The fraud case of Wells Fargo revealed the danger of companies putting high-pressure sales quotas on employees. The result of such a practice at Wells Fargo Bank led hundreds of its employees to open fake accounts for Wells Fargo clients.

Short-term profits went up by millions, but when the widespread fraud was uncovered, the bank's fine imposed by the Securities and Exchange (SEC) ran into the billions. In addition, the bank lost hundreds, if not thousands, of clients.

Fraud Risk Management

17.2

Fraud is a deliberate act (or failure to act) to obtain an unauthorized benefit, either for oneself or for the institution, by using deception or false suggestions or suppression of truth, or other unethical means, which are believed and relied upon by others. Depriving another person or the institution of a benefit to which he/she is entitled by sharing any of the means described above also constitutes fraud.

Examples of fraudulent acts include, but are not limited to, the following:

- Embezzlement.
- Forgery or alteration of documents.
- Unauthorized alteration or manipulation of computer files.
- Fraudulent financial reporting.
- Misappropriation or misuse of resources (e.g., funds, supplies, equipment, facilities, services, inventory, or other assets).
- Authorization or receipt of payment for goods not received or services not performed.
- Authorization or receipt of unearned wages or benefits.
- Conflict of interest, ethics violations.

Fraud Triangle:

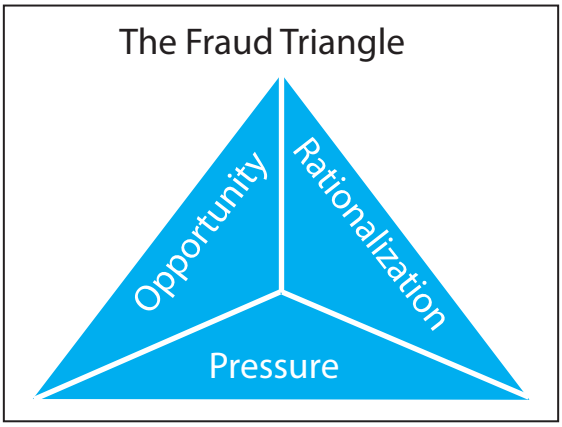

Figure 17.1: Fraud Triangle

Employees who commit fraud generally can do so because there is an opportunity, pressure, and rationalization.

(a) Opportunity is generally provided through weaknesses in the internal controls.

Some examples include inadequate or no:

- Supervision and review.
- Separation of duties.
- Management approval.
- System controls.

(b) Pressure (or motive) can be imposed due to:

- Personal financial problems; unforeseen expenses.
- Personal vices/addictions such as gambling, drugs, shopping, etc.
- Unrealistic deadlines and performance goals.

(c) Rationalization occurs when the individual develops a justification for their fraudulent activities. The rationalization varies by case and individual.

Some examples include:

- "I need this money and I'll pay it back when I get my pay check other people are doing it."
- "I didn't get a raise. The University owes me."

Breaking the Fraud Triangle is the key to fraud deterrence. Breaking the Fraud Triangle entails removing one of the elements in the fraud triangle to reduce the likelihood of fraudulent activities. "Of the three elements, removal of Opportunity is most directly affected by the system of internal controls and generally provides the most actionable route to deterrence of fraud" (Cendrowski, Martin, Petro, The Handbook of Fraud Deterrence).

Red Flags for Fraud:

Managers and employees are responsible and should be aware of the red flags for fraud. These are warning signs that may indicate that fraud risk is higher without any evidence that fraud occurring. The existence of one or two flags is not something to be overly concerned about. However, if multiple flags are present and accounting irregularities or weak controls are identified, then the Internal Audit department should be contacted.

Examples of red flags include, but are not limited to, the following:

Employee Red Flags:

- Employee lifestyle changes: expensive cars, jewellery, homes, clothes.
- Significant personal debt and credit problems.
- Behavioural changes- These may be an indication of drugs, alcohol, gambling, or just fear of losing the job.
- High employee turnover, especially in those areas which are more vulnerable to fraud.
- Refusal to take a vacation or sick leave.
- Lack of segregation of duties in a vulnerable area.

Management Red Flags:

- Management frequently overrides internal controls.
- Management decisions are dominated by an individual or small group.
- Managers display significant disrespect for regulatory bodies.

- Policies and procedures are not documented or enforced.
- Weak internal control environment.
- Accounting personnel is lax or inexperienced in their duties.
- Decentralization without adequate monitoring.
- An excessive number of checking accounts; frequent changes in banking accounts.
- An excessive number of year-end transactions; unnecessarily convoluted transactions.
- High employee turnover rate; low employee morale.
- Refusal to use serial numbered documents (receipts).
- The compensation program is out of proportion.
- Photocopied or missing documents.
- Reluctance to provide information to, or engage in frequent disputes with, auditors.
- Frequent Changes in banking accounts
- Frequent Changes in external auditors
- Company Assets are sold at a value which is below market value

Suspect Fraud or Misconduct:

Any employee who suspects that dishonest, unethical, or fraudulent activity is occurring should not attempt to personally contact the suspected individual to determine facts, conduct investigations or interviews /interviews interrogations taken to avoid mistaken accusations or alert suspected individuals that an investigation may be under way.

An underway Corporate Scandals

Corporate scandals and frauds in India are as old as the hills. The 1950s witnessed the infamous Life Insurance Corporation / Mundhra scam, which was the first major financial fraud in independent India. Frauds continued with an alarming regularity thereafter in every decade – the infamous Harshad Mehta, Ketan Parekh, Sahara, and Satyam scams are just a few of them. These frauds were investigated by the law enforcement agencies under the relevant provisions of the Indian Penal Code, 1860 (**IPC**). The Companies Act, 1956 did not have any separate definition of 'fraud'. Legally, it was not necessary to have a separate one as Lord Macaulay's IPC adequately dealt with all such crimes. The Companies Bill, 2008 was the original legislative proposal to replace the Companies Act, 1956 basis Dr. J.J. Irani Committee Report (**Irani Report**). The Irani report did not have any recommendation for a provision like Section 447 dealing with frauds. It seems the intervening major corporate scandals of 2007-08 led the Parliamentary Standing Committee to recommend two new legislative changes:

1. Separate definition of fraud under Section 447 of the Companies Act, 2013 (**the Act**) and
2. Creation of the Serious Fraud Investigation Office (**SFIO**) under Section 212 of the Act to investigate those frauds.

Section 447 of the Act is an amalgam of several sections of the IPC including Section 405 dealing with Criminal Breach of Trust, Section 415 dealing with Cheating, Section 463 dealing with Forgery, and Section 477A dealing with falsification of accounts.

Definition of Fraud under Section 447 of the Act:

Section 447 of the Act starts with the words "without prejudice to any liability including repayment of any debt under this Act or any other law" which means without affecting adversely any other legal proceedings. In the context of the said section, it signifies that the proceedings initiated under Section 447 of the Act will not be barred provided they do not adversely affect an action or a proceeding relating to any liability. This includes repayment of debt initiated under any other provision of the Act or any other law for the time being in force.

As per the explanation, the various elements of fraud include:

(a) Any act, or

(b) Omission, or

(c) Concealment of any factor

(d) Abuse of position

Committed by any person or any other person with the connivance in any matter, with the **intent to deceive**, or to gain undue advantage from, or to injure the interests of the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.

The term '**Intent to Deceive'** has been judicially examined from the perspective of Section 463 of IPC. It was held in the case of Vimla v. State that the idea of deceit is a necessary ingredient of fraud, but it does not exhaust it. The expression 'defraud' involves two elements, namely, deceit and injury to the person deceived. Injury is something other than the economic loss that is deprivation of property, whether movable or immovable or of money and it will include any over caused to any person in body, mind, reputation or, such others. A benefit or advantage to the deceiver will almost cause a loss or detriment to the deceived. Even in those rare cases where there is a benefit or advantage to the deceiver, but no corresponding loss to the deceived, the second condition is satisfied.

Section 447 of the Act has been invoked in a few recent corporate scandals which are still at different stages of the trial. Given that it is a relatively new provision, there are no direct pronouncements on this provision so far either by National Company Law Tribunal (NCLT) or the High Courts, or the Supreme Court (SC). This provision has been invoked by the Serious Fraud Investigation Office (SFIO) in a few recent corporate scandals.

The Act has introduced stringent punishment for persons who are found to be guilty of fraud. Fraud, if it involves an amount of at least INR 10 lakh or 1% of the turnover of the company, whichever is lower, is an offenseable by imprisonment not less than six months and can go up to a maximum of 10 years. The provision for a fine cannot be less than the amount of fraud and may extend up to three times the fraud amount. However, if the fraud in question involves public interest, the term of imprisonment shall not be less than three years.

The offense under Section 447 of the Act is cognizable, non-bailable, and non-compoundable.

Section 446A of the Act lays down five factors to be considered by the Court while deciding the amount of fine or imprisonment under the Act: (a) size of the company; (b) nature of business carried on by the company; (c) injury to the public interest; (d) nature of the default; and (e) repetition of the default.

Standard of Proof:

Section 447 of the Act provides for maximum imprisonment for five years. The standard of proof is 'beyond reasonable doubt'. Recently, the SC in the matter of the Latest State of Maharashtra explained the term 'reasonable doubt' as "a mean between excessive caution and excessive indifference to a doubt, further it has been elaborated that reasonable doubt must be a practical one and not an abstract theoretical hypothesis…"

Reporting Duty of the Auditors:

Section 143(12) of the Act casts an obligation upon the auditors of companies to report to the Central Government about fraud or suspected fraud committed against a company by its officers or employees. Further, if the auditor does not report fraud as provided above wi receive the regulators, the auditor can be deemed to have committed fraud himself and be removed under the provisions of Section 140(5) of the Act.

Latest Developments:

SEBI has amended the SEBI (Listing Obligations and Disclosure Requirements-LODR) Regulations, 2015 with effect from October 08, 2020, to provide that in case of initiation of a forensic audit, (by whatever name called), the following disclosures shall be made to the stock exchanges by the listed entities:

1. The fact of initiation of forensic audit along-with name of entity initiating the audit and reasons for the same, if available;
2. Final forensic audit report (other than for forensic audit initiated by regulatory / enforcement agencies) on receipt by the listed entity along with comments of the management, if any.

This new requirement to report is without any materiality thresholds, which could cause a high level of anxiety to the Audit Committee and Boards as any such disclosure could have a profound impact on the stock price of the company. In addition, speculative reporting by the media may also create panic among the investor community.

Several recent corporate frauds seem to have alarmed lawmakers and the latest tightening of Sections 447 and 212 of the Act, coupled with the inclusion of fraud as an offence under the PMLA, has alarmed the Audit Committees and the Corporate Boards. Stringent conditions for the grant of bail, provisions for disgorgement of assets, claw-back of remuneration, and unlimited personal liability of directors have further damaged the frayed nerves of independent directors. Regulators and the enforcement agencies are increasingly becoming prosecuting new requirements for reporting to the stock exchange, even the commencement of a forensic audit may create further complications every time a whistle blower complaint is received by the Audit Committee. Independent directors now prefer to undertake comprehensive due diligence of compliance and the governance standards of a company before accepting new board positions. India Inc. is slowly adapting itself to the new normal.

Financial Forensics and Forensic Audit Techniques

17.3

Financial forensics is a field that combines accounting and investigation. One of the main purposes of financial forensics is discovering and gathering evidence of criminal activity involving money. They investigate individuals' and organisations' finances to determine the truth about how they manage them. Financial forensics professionals help prevent financial crime and recover lost assets.

Financial forensics professionals also work with investors to find investment opportunities.

The financial forensics professional, or forensics financial analyst, researches other businesses to determine their true value.

Examples of common cases a financial forensics professional might work on:

Financial theft: Financial theft occurs when a customer, an employee, or another individual steals money from an organisation. An employee, for example, might take money from a cash register. A financial forensics analyst studies the event, looking for evidence of theft in documents such as receipts, payments or profit-or-loss statements.

Securities fraud: Securities fraud is a type of white-collar crime that typically occurs when someone presents false information to an investor. For example, a stockbroker might give misleading advice to convince a client to invest in a certain company. Both individuals and organisations, such as investment banks and brokerage firms, can commit securities fraud. A financial forensics professional searches through documents such as stock transactions and communication records to determine if someone committed securities fraud.

Money laundering: Money laundering is the process of making money earned through illegal methods look legal. For example, someone might take stolen cash and invest it into a cash-based business, such as a restaurant. The restaurant deposits both its legal profits and the illegal cash into a financial institution, allowing it to use the illegal funds. To detect money laundering, a financial forensics analyst might research shell company documentation, significant changes in income at cash-based businesses, and inexplicable or suspicious transactions.

Corporate valuation disputes: A financial forensics professional might analyse a business to determine its value. For example, if one business is acquiring another, it might want to know the exact value of that organisation. Using a forensic analyst, they can learn more about that organisation's finances than what's available publicly. This helps ensure they're buying the business at a fair price and that it has no hidden financial issues.

Tax evasion: Tax evasion occurs when a person or organisation avoids paying their taxes. For example, a company might try to hide profits in a shell corporation so they don't have to pay taxes on it. A forensics analyst studies tax documents, profit-and-loss statements, and financial transactions to determine if someone committed tax evasion.

Forensic Audit Techniques:

In recent years, there have been considerable changes in the business landscape. The increasing globalization, free movement of people, easy communication, technological advancements, and the shrinking of the world have

helped change the business environment. These factors have led to the rapid growth of established businesses and the sprouting of new ones. However, this growth of companies has also increased in financial crimes and frauds.

Many businesses keep a separate department of in-house accountants who keep an eye on all the business activities and strive to minimize any irregularities in the business's recordings. However, there are still cases of new and innovative fraudulent activities that can only be uncovered after an in-depth analysis of all the records and books of the business.

This situation has led to the growth of a niche field known as forensic accounting, which can be explained as the integration of accounting and investigative skills. To understand more about forensic accounting and the various techniques which help in uncovering any financial fraud.

Forensic Accounting/Auditing is a type of accounting that cross-checks a business's various financial records to find any indication of fraud being committed. It also provides an in-depth analysis of all of the business›s financial books, which could be presented in the court of law as evidence. Forensic accountants can be considered detectives in the economic and business field. These people go through every recorded transaction and try to find any fraudulent or illegal activity within the industry.

Forensic accounting not only helps the business minimize its losses but will also help improve the efficiency of the business, ultimately leading to greater profitability. Furthermore, it can help the management keep track of the various business activities and prevent any fraud from happening in the future.

Qualities a Forensic Accountant Should Have:

Here are some qualities which a forensic accountant should possess. These are only some of the traits and not an exhaustive list. More qualities can be added to this list.

- Have a Logical Mind.
- Give attention to detail.
- Give value to Moral Principles.
- Question Everything/Inquisitiveness
- Be Spontaneous.
- Good understanding of Accounting transactions and impacts.

Having these qualities will provide forensic accountants with an urge to dig deeper and will make them a very successful forensic accountant. With proper investigative techniques added to the mix, the accountants would be capable of digging out even the most minute discrepancy in the accounting records.

The investigative techniques for forensic accounting:

There are several techniques for conducting a forensic review of the business. The ones provided below are generic but effective. These are the forensic techniques that apply to almost all companies. These are:

Reviewing Public Documents and Conducting Background Checks:

The documents made available to the public are scrutinized as they are the easiest to obtain. Also, thorough background checks of a particular company are done to see the past dealings of the business. Public Documents would include any information in the public database, the corporate records, and any legally available information on the internet.

Conducting Detailed Interviews:

Conducting an interview is an essential technique that can transform an unwilling person into a source of valuable information. It helps in fully understanding all the facts. An interview should be conducted by accurately assessing the gravity of the situation and preparing the questions according to it. Discussions should take every detail into account and look at the greater picture to figure out the magnitude of the illegal activity and the culprit responsible.

Gathering Information from Trustworthy Sources:

Information provided by a confidential and trustworthy source can be precious to any case. When a piece of information is gained from a confidential source or a confidential informant, all the necessary precautions should be taken to hide the identity of the so-called cause. A forensic accountant should try to have as many confidential sources as possible because such sources can virtually guarantee a correct result.

Analysing Evidence Gathered:

Proper analysis of the obtained evidence can point to the guilty party and assist in understanding the extent of the fraud committed in the business. Furthermore, this analysis would also help understand how secure the company is against financial scams and installing various austerity measures to prevent any such future situation.

Conducting Surveillance:

This can be done physically or electronically and is one of the conventional measures to uncover any fraud. It can be done by monitoring and tracking all the official emails and messages.

Going Undercover:

This is an extreme measure and should be used only as a last resort. It is best left to the professionals as they know how and where to conduct the investigations. Even a small mistake while being undercover can signal the offender that something is wrong, and the person might vanish/disappear from the scene.

Analysing the Financial Statements:

This is a special tool for finding out the fraud committed. All the necessary details are summarised in the financial statement, and the analysis of these statements can help a forensic accountant figure out the scam.

Nowadays, the economic conditions are getting stricter, and each country's government is now implementing tighter laws regarding the governance of the businesses. As the companies are increasing the level of sophistication, so is fraud. This has led to a higher sensitivity to fraud which can be interpreted as massive demand for the services of forensic accountants by all the businesses.

Ethical Considerations and Code of Conduct in Forensic Audit

17.4

Ethical issues in business can be a difficult challenge to navigate for any business owner. Though some laws and statutes exist to hold workers and employers accountable, these alone do not entirely deter employees from behaving unethically.

Ethical Issues in Business

Ethical issues in business encompass a wide array of areas within an organisation's ethical standards. Fundamental ethical issues in business include promoting conduct based on integrity and trust, but more complex issues include accommodating diversity, empathetic decision-making, and compliance and governance that is consistent with the organisation's core values. According to the Global Business Ethics Survey of 2019, 25% of employees still feel that their senior managers do not have a good understanding of key ethical and compliance business risks across the organisation.

To manage the ethical issues in business that arise in an organisation, first need to develop a thorough understanding of what those issues can look like. Understanding how to detect and, most importantly, deter these issues before they become a problem can ensure to focus stays on business growth and success instead of remediation.

Harassment and Discrimination in the Workplace

Harassment and discrimination are arguably the largest ethical issues that impact business owners today. Should harassment or discrimination take place in the workplace, the result could be catastrophic for the organisation both financially and reputationally.

Every business needs to be aware of the anti-discrimination laws and regulations that exist to protect employees from unjust treatment. The U.S. Equal Employment Opportunity Commission (EEOC) defines many different types of discrimination and harassment statutes that can affect organisations, including but not limited to:

Age: Applies to those 40 and older, and to any ageist policies or treatment that takes place.

Disability: Accommodations and equal treatment are provided within reason for employees with physical or mental disabilities.

Equal Pay: Compensation for equal work regardless of sex, race, religion, etc.

Pregnancy: Accommodations and equal treatment are provided within reason for pregnant employees.

Race: Employee treatment is consistent regardless of race or ethnicity.

Religion: Accommodations and equal treatment are provided within reason regardless of employee religion.

Sex and Gender: Employee treatment is consistent regardless of sex or gender identity.

Health and Safety in the Workplace:

As outlined in the regulations stipulated by the Occupational Safety and Health Administration (OSHA), employees have a right to safe working conditions. According to their 2018 study, 5,250 workers in the United States died from occupational accidents or work-related diseases. On average, that is more than 100 a week, or more than 14 deaths every day. The top 10 most frequently cited violations of 2018 were:

Fall Protection, e.g., Unprotected sides and edges and leading edges.

Hazard Communication, e.g., Classifying harmful chemicals.

Scaffolding, e.g., Required resistance and maximum weight numbers.

Respiratory Protection, e.g., Emergency procedures and respiratory/filter equipment standards.

Lockout / Tagout, e.g., Controlling hazardous energy such as oil and gas.

Powered Industrial Trucks, e.g., Safety requirements for fire trucks.

Ladders, e.g., Standards for how much weight a ladder can sustain.

Electrical, Wiring Methods, e.g., Procedures for how to circuit to reduce electromagnetic interference.

Machine Guarding, e.g., Clarifying that guillotine cutters, shears, power presses, and other machines require a point of operation guarding.

Electrical, General Requirements, e.g., Not placing conductors or equipment in damp locations.

However, health and safety concerns should not be limited to physical harm. In a 2019 report conducted by the International Labour Organization (ILO), an emphasis was placed on the rise of "psychosocial risks" and work-related stress and mental health concerns. Factors such as job insecurity, high demands, effort-reward imbalance, and low autonomy, were all found to contribute to health-related behavioural risks, including sedentary lifestyles, heavy alcohol consumption, increased cigarette smoking, and eating disorders.

Whistle blowing or Social Media Rants

The widespread nature of social media has made employees' conduct online a factor in their employment status. The question of the ethics of firing or punishing employees for their online posts is complicated. However, the line is usually drawn when an employee's online behaviour is considered to be disloyal to their employer. This means that a Facebook post complaining about work is not punishable on its own but can be punishable if it does something to reduce business.

In the same vein, business owners must be able to respect and not penalize employees who are deemed whistle-blowers to either regulatory authorities or on social media. This means that employees should be encouraged, and cannot be penalized, for raising awareness of workplace violations online. For example, a Yelp employee published an article on the blogging website Medium, outlining what she claimed as the awful working conditions she was experiencing at the online review company. She was then fired for violating Yelp's terms of conduct. The ambiguity of her case, and whether her post was justifiable, or malicious and disloyal conduct, shows the importance of implementing clear social media policies within an organisation. To avoid this risk of ambiguity, a company should stipulate which online behaviours constitute an infringement.

Ethics in Accounting Practices

Any organisation must maintain accurate bookkeeping practices. "Cooking the books", and otherwise conducting unethical accounting practices, is a serious concern for organisations, especially publicly traded companies.

An infamous example of this was the 2001 scandal with American oil giant Enron, which was exposed for inaccurately reporting its financial statements for years, with its accounting firm Arthur Andersen signing off on statements despite them being incorrect. The deception affected stockholder prices, and public shareholders lost over $25 billion because of this ethics violation. Both companies eventually went out of business, and although the accounting firm only had a small portion of its employees working with Enron, the firm's closure resulted in 85,000 jobs lost.

In response to this case, as well as other major corporate scandals, the U.S. Federal Government established the Sarbanes-Oxley Act in 2002, which mandates new financial reporting requirements meant to protect consumers and shareholders. Even small privately held companies must keep accurate financial records to pay appropriate taxes and employee profit-sharing, or to attract business partners and investments.

Non-disclosure and Corporate Espionage

Many employers are at risk of current and former employees stealing information, including client data used by organisations in direct competition with the company. When intellectual property is stolen, or private client information is illegally distributed, this constitutes corporate espionage. Companies may put in place mandatory non-disclosure agreements, stipulating strict financial penalties in case of violation, to discourage these types of ethics violations.

Technology and Privacy Practices

Under the same umbrella as non-disclosure agreements, the developments in technological security capability pose privacy concerns for clients and employees alike. Employers now can monitor employee activity on their computers and other company-provided devices, and while electronic surveillance is meant to ensure efficiency and productivity, it often comes dangerously close to privacy violations.

2019 survey conducted by the American Management Association, 66% of organisations were found to monitor internet connections, with 45% tracking content, keystrokes, and time spent on the keyboard, and 43% storing and reviewing computer files as well as monitoring employee emails. The key to ethically using technological surveillance is transparency. According to the same survey, 84% of those companies tell their employees that they are reviewing computer activity. For employee surveillance does not turn into an ethical issue for business, both employees and employers should remain conscious of the actual benefits of being monitored, and whether it is a useful way of developing a record of their job performance.

Ethical Issues in Business

Avoiding ethical issues in business always starts with top management. Providing written policies and processes that ensure those policies are both acknowledged and adhered to, can ensure transparency and ethical business practices are applied.

To effectively detect and, most importantly, deter ethical issues in business from surfacing in an organisation, several everyday efforts take. Be sure to communicate and enforce a robust code of ethics when making decisions and ask the same of employees. Remain aware of the discrimination laws that exist in the region. Stay informed on the rules that impute and the story and ensure the organisation is acting in compliance with those regulations. Collaborate with accountants, maintaining transparency and honesty in financial the ports. Be presenting company, making sure organisation and employees alike are always doing the right and ethical thing.

Auditors

To bound auditors around the world to achieve objectives of engagement effectively and also provide users of financial statements with reasonable assurance and make responsible for other aspects of the professionals have to abide by the requirements of ethics. Principles laid out in the code of ethics are also known as fundamental ethical

principles the auditor is required to assure all such principles are fulfilled. Fundamental principles include honesty or integrity**,** objectivity**,** professional competence, due care, and professional behaviour**.**

However, during the practice, while carrying requirements of engagement auditors may face or expect to face such situations when they will not be able to fulfil the requirements. Such obstructions are called threats to fundamental principles. Although threats can make many different shapes broadly, they can be classified into various categories:

Self-interest threat arises when the stake of the total stake of any immediate or close family member of the auditor is involved in the entity and thus, he might cause the auditor to violate multiple ethical requirements.

Advocacy threat arises when the auditor (most of the time unintentionally) supports the opinion or position (of the client most of the time) to the extent that it is not supported with relevant evidence or simply auditor supported the opinion beyond the degree of objectivity.

Intimidation threat arises when the auditor, directly or indirectly, is threatened physically or mentally to keep him from working objectively.

For example, Auditor is given a threat that if he reports objectively then the audit fee will not be paid or subsequent audits with the auditor will be cancelled. It might take the shape of physical threats like harming family members or the use of coercion on the auditor.

The company's good name and the trust of stakeholders are two of its most important assets. Protect the company's reputation and increase employee engagement by creating a workplace where ethical conduct is the norm.

Reduce ethics risk by taking these five key steps:

- Honestly assess needs and resources.
- Establish a strong foundation.
- Build a culture of integrity from the top down.
- Keep a "values focus" in moments big and small.
- Re-evaluate and revise as needed.

Honestly assess needs and resources

Successful businesses start with a good plan. So do successful ethics and compliance programs. To create a relevant and meaningful plan, have to know the law of the land. It's important to know:

- What ethics challenges are common in the work we do? In our workplace?
- Where are our greatest areas of risk? Which groups of employees, locations, business units, etc. are potential "hot spots"?
- What values are important to our company and its employees?
- What values are necessary for our business, our work in particular?
- What ethics and compliance resources will be most beneficial for employees? What vehicles of support (a phone line, an email, an individual or committee, an internal social network, etc.) are likely to be most utilized and helpful?
- In developing our code and values, which groups' input is necessary? Who would be helpful?

Plan/program will only make a difference if Management begins having an accurate picture of existing strengths and areas of vulnerability. Risk assessment should be the starting point of internal efforts, followed by gap analysis and program assessment. Audit reports are also an essential piece of the puzzle.

The company can gather information in a variety of ways. Focus groups allow representative samples of the larger population to share their opinions and experiences; they provide a deep, rich "snapshot" of the state of ethics in the organisation. Surveys (internal or conducted by a third party) provide the opportunity to gather information from a much larger group of employees see to compare results, and analyse by relevant subgroups (i.e., employee levels, departments, units, etc.).

Strong Foundation:

Written Standards of Ethical workplace conduct:

- Training on the standards.
- Company resources that provide advice about ethics and compliance issues.
- A means to report potential violations confidentially or anonymously.
- Performance evaluations of ethical conduct.
- Systems to discipline violators.

But just having these elements is not enough. When it comes to ethical conduct and compliance, it's not enough to "print, post, and pray". Implementation and integration matters.

Company ethics and compliance programs must be a vital, integrated element of work and the two way you it, ensuring that employees know how to and feel supported in their efforts to uphold ethics and compliance standards in their work. The hallmarks of an effective ethics and compliance program are:

- Freedom to question management without fear;
- Rewards for following ethics standards;
- Not rewarding questionable practices, even if they produce good results for the company;
- Positive feedback for ethical conduct;
- Employee preparedness to address misconduct; and
- Employees' willingness to seek ethics advice.

Develop a Culture of Integrity:

People have an innate desire to get along and (long-past high school) want to fit in and conform to the norms of those around them. It may not be pleasant to admit it, but most people's ethics standards are fairly malleable. Although most people retain a desire to "do the right thing," the definition of right is significantly influenced by the company they keep. Culture matters.

Fortunately, if the company has diligently built an ethics and compliance program and woven it into the daily operations of the organisation, a strong ethics culture is far more likely. Research proves that an effective ethics and compliance program helps build a culture of integrity in which everyone "walks the talk". In a strong ethics culture, employees at all levels are committed to doing what is right and upholding values and standards.

Leaders are powerful drivers of corporate culture; they set the tone in any organisation. They decide who gets attention, who gets promoted, and what merits rewards and recognition. They set the standard. There are several things' leaders should do to help promote a strong ethics culture:

- Talk about the importance of ethics.
- Keep employees adequately informed about issues that impact them.

- Uphold promises and commitments to employees and stakeholders.
- Acknowledge and reward ethical conduct.
- Hold accountable those who violate standards, especially leaders.
- Model ethical conduct both professionally and personally.

When it comes to ethical leadership, there are two key things to keep in mind:

Character is paramount: Ethical leaders show integrity not only in the way they conduct themselves at work but in their relationships as well. In a world of social media, private behaviour comes public knowledge, and shapes employees' beliefs about what kind of individuals their leaders are.

Leadership happens at all levels: While senior leaders set the tone for the entire organisation, supervisors shape the everyday environments in which employees work and make decisions. The actions of supervisors have a profound impact on employees and their workplace conduct.

Keep a "Values Focus":

Ethics is about choices-big and small. Organisations with integrity keep their values at the forefront in both mundane and extraordinary moments. Corporate values should come into play and be reflected in multiple processes that drive the everyday life of the company, including:

- HR policies and their implementation.
- Reward systems.
- Hiring and retention.
- Performance management and evaluation.
- Promotion decisions.

On those occasions when crises occur, leaders should recognize not only the ethical dimension of the moment at hand but the "teachable moment" it represents. Edgar Schein, the father of the study of organisational culture, noted that moments of crisis are particularly powerful culture-builders because of the intensity of emotion involved. Employees learn a great deal about leaders' priorities and character when they show their "True Colours." If leaders make values their touchstone in times of crisis, employees learn that ethics matters.

Re-evaluate and Revise:

Situations and needs will change. Employees need to know what is working, what isn't, what new vulnerabilities have emerged, what progress made, and where there's work yet to be done. Be disciplined about regularly revisiting the state of ethics and compliance in the organisation. Risk assessments, follow-up surveys, and periodic or ongoing focus groups will allow the program to relevant and regular assessments will demonstrate internally (and, if ever needed, externally) that the resources in ethics and compliance have made a difference.

Major Threats in Auditing Profession:

In the auditing profession, **major threats** may compromise an auditor's independence. Before an audit engagement, it is each member of the audit team must review five threats to independence. If an auditor is exposed to a certain threat, he or she should either develop safeguards to reduce the threat to an acceptable level or resign from the audit engagement.

The following are that can potentially compromise the independence of auditors:

Self-Interest Threat: A self-interest threat exists if the auditor holds a direct or indirect financial interest in the company or depends on the client for a major fee that is outstanding.

Example: The audit team is preparing to conduct its 2020 audit for ABC Company. However, the audit team has not received its audit fees from ABC Company for its 2019 audit.

Issue: The audit team might be tempted to issue a favourable report so that the company can secure a loan to settle the fees outstanding for their 2019 audit.

Self-Review Threat: A self-review threat exists if the auditor is auditing his work or work that is done by others in the same firm.

Example: The auditor prepares the financial statements for ABC Company while also serving as the auditor for ABC Company.

Issue: By having the auditor review his or her work, the auditor cannot be expected to form an unbiased opinion on the financial statements.

Advocacy Threat: An advocacy threat exists if the auditor is involved in promoting the client, to the point where their objectivity is potentially compromised.

Example: The auditor is assisting in selling ABC Company while also serving as the auditor for the company.

Issue: The auditor may issue a favourable report to increase the sale price of ABC Company.

Familiarity Threat: A familiarity threat exists if the auditor is too personally close to or familiar with employees, officers, or directors of the client company.

Example: ABC Company has been audited by the same auditor for over 10 years and the auditor regularly plays golf with the CEO and CFO of ABC Company.

Issue: The auditor may have become too familiar with the client and, thus, lack objectivity in their work.

Intimidation Threat: An intimidation threat exists if the auditor is intimidated by management or its directors to the point that they are deterred from acting objectively.

Example: ABC Company is unhappy with the conclusion of the audit report and threatens to switch auditors next year. ABC Company is the biggest client of the auditor.

Issue: The auditor's independence may be compromised, as ABC Company is their biggest client and they, quite naturally, do not want to lose such a client. Therefore, the auditor may issue a report that appeases ABC Company.

Most companies have some form of ethics policy in place. The name of the policy may vary. Some companies call them Code of Ethics, Code of Conduct, or just plain Ethics Policy, but they all have the same goal: to ensure all employees behave ethically.

Companies create this policy for good reasons. They want to make sure their employees behave ethically and have a clear outline of the expectations and consequences of violations, but having a policy in place doesn't mean it is effective. In most the companies, despite having a formal ethics policy in place that supposedly protected whistle-blowers, many employees were fired for calling the hotline to report the fraud they were being ordered to commit.

There are three primary challenges companies face when implementing an effective ethics policy:

Resistance from employees: The first challenge is resistance from employees. Not because employees are inherently unethical or immoral, but when they are facing a new ethics policy, they may be made to feel that way. Companies should offer as much communication as possible to let employees know why the policy is being implemented and how it affects them.

One way to ease the resistance is to make sure to implement a values-driven policy. A values-driven ethics policy will be more warmly welcomed by employees, thanks to its focus on the values and reasons behind the policy instead of the consequences of non-compliance.

Costs of training and other implementation fees can be high: The cost of creating an ethics policy is minimal. However, the cost of implementing and maintaining an effective ethics policy is much higher. An ethics policy is worthless if no one understands it. That's why companies must train their employees in ethics regularly. All employees should be subject to training, from the CEO to the newest hire, but not all training is equal.

Training programs should be tailored to employees as much as possible. Employees in one department may face very different ethical dilemmas than employees in another. Customize training whenever possible to ensure employees understand the full measure of the ethics policy.

Inability to determine ROI of the ethics policy: It is notoriously difficult for executives to demonstrate ROI in ethics programs, pointed out in Wall Street Journal article. "ROI is hard to measure for a couple of reasons: it's not easy to measure a lack of wrongdoing, and it's not obvious what success looks like for some of the outcomes. For example, is higher or lower call volume on integrity hotline more desirable?"

However, he goes on to mention that the connection of ethics and compliance programs to performance and corporate strategy is one way to increase the likelihood of having demonstrable ROI. That's why companies should focus on the long-term value of the ethics policy.

Of course, the real key to implementing an effective ethics policy has quality ethical leaders at the top. Most ethics experts agree that senior management must set the tone for integrity and ethical behaviour to establish a solid foundation for the rest of the company. Confidence in ethical leadership will encourage all employees to follow and abide by the ethics policy.

Code of Conduct in Forensic Audit:

The Association of Certified Fraud Examiners is an association of professionals committed to performing at the highest level of ethical conduct. Auditors of the Association pledge themselves to act with integrity and to perform their work professionally.

Auditors have a professional responsibility to their clients, to the public interest, and each other; a responsibility that requires subordinating self-interest to the interests of those served.

These standards express basic principles of ethical behaviour to guide Auditors in fulfilling of their duties and obligations. By following these standards, all Certified Fraud Examiners shall be expected, and all Associate Auditors shall strive to demonstrate their commitment to excellence in service and professional conduct.

Applicability of Code:

The CFE Code of Professional Standards shall apply to all Certified Auditors of the Association of Certified Fraud Examiners ("ACFE"). Associate Auditors of the ACFE should strive to adhere to the Standards but are not bound by them. The use of the terms "Certified Fraud Examiner" or "CFE" in this Code shall refer to certified Auditors.

Standards of Professional Conduct

A. Integrity and Objectivity:

1. Certified Fraud Examiners shall conduct themselves with integrity, knowing that public trust is founded on integrity. CFEs shall not sacrifice integrity to serve the client, their employer, or the public interest.
2. Before accepting the fraud examination, Certified Fraud Examiners shall investigate for actual or potential conflicts of interest. CFEs shall disclose any actual or potential conflicts of interest to prospective clients who retain them or to their employers.

3. Certified Fraud Examiners shall maintain objectivity in discharging their professional responsibilities within the scope of the engagement.
4. Certified Fraud Examiners shall not commit acts discreditable to the ACFE or its Auditor ship, and shall always conduct themselves in the best interests of the reputation of the profession.
5. Certified Fraud Examiners shall not knowingly make a false statement when testifying under oath in a court of law or another dispute resolution forum. CFEs shall comply with lawful orders of the courts or other dispute resolution bodies. CFEs shall not commit criminal acts or knowingly induce others to do so.

B. Professional Competence:

1. Certified Fraud Examiners shall be competent and shall not accept assignments where competence is lacking.

   In some circumstances, it may be possible to meet the requirement for professional competence by use of consultation or referral.
2. Certified Fraud Examiners shall maintain the minimum program of continuing professional education required by the Association of Certified Fraud Examiners. A commitment to professionalism combining education and experience shall continue throughout the CFE's professional career. CFEs shall continually strive to increase the competence and effectiveness of their professional services.

C. Due Professional Care:

1. Certified Fraud Examiners shall exercise due professional care in the performance of their services. Due professional care requires diligence, critical analysis, and professional skepticism in discharging professional responsibilities.
2. Conclusions shall be supported with evidence that is relevant, competent, and sufficient.
3. Fraud examinations shall be adequately planned. Planning controls the performance of a fraud examination from inception through completion and involves developing strategies and objectives for performing the services.
4. Work performed by assistants and other professionals operating under the Certified Fraud Examiner's direction on a fraud examination shall be adequately supervised. The extent of supervision required varies depending on the complexities of the work and the qualifications of the assistants or professionals.

D. Understanding with Client or Employer:

1. At the beginning of a fraud examination, Certified Fraud Examiners shall reach an understanding with those retaining them (client or employer) about the scope and limitations of the fraud examination and the responsibilities of all parties involved.
2. Whenever the scope or limitations of a fraud examination or the responsibilities of the parties change significantly, a new understanding shall be reached with the client or employer.

E. Communication with Client or Employer:

Certified Fraud Examiners shall communicate to those who retained them (client or employer) significant findings made during the normal course of the fraud examination.

F. Confidentiality:

Certified Fraud Examiners shall not disclose confidential or privileged information obtained during the fraud examination without the express permission of proper authority or the lawful order of a court. This requirement

does not preclude professional practice or investigative body reviews as long as the reviewing organisation agrees to abide by the confidentiality restrictions.

Standards of Examination:

A. Fraud Examinations:

1. Fraud examinations shall be conducted in a legal, professional, and thorough manner. The Certified Fraud Examiner's objective shall be to obtain evidence and information that is complete, reliable and relevant.
2. Certified Fraud Examiners shall establish prediction and scope priorities at the outset of a fraud examination and continuously re-evaluate them as the examination proceeds. CFEs shall strive for efficiency in their examination.
3. Certified Fraud Examiners shall be alert to the possibility of conjecture, unsubstantiated opinion, and bias of witnesses and others. CFEs shall consider both exculpatory and inculpatory evidence.

B. Evidence:

1. Certified Fraud Examiners shall endeavour to establish effective control and management procedures for documents, data, and other evidence obtained during an examination. CFEs shall be cognizant of the chain of custody including origin, possession, and disposition of relevant evidence and material. CFEs shall strive to preserve the integrity of relevant evidence and material.
2. Certified Fraud Examiners' work may vary with the circumstances of each fraud examination. The extent of documentation shall be subject to the needs and objectives of the client or employer.

Standards of Reporting:

A. General:

1. Certified Fraud Examiners' reports may be oral or written, including fact witness and/or expert witness testimony, and may take many different forms. There is no single structure or format that is prescribed for a CFE's report; however, the report should not be misleading.

B. Report Content:

1. Certified Fraud Examiners' reports shall be based on evidence that is sufficient and relevant to support the facts, conclusions, opinions, and/or recommendations related to the fraud examination. The report shall be confined to subject matter, principles, and methodologies within the member's area of knowledge, skill, experience, training or education.
2. No opinion shall be expressed regarding the legal guilt or innocence of any person or party.

Code of Ethics for Certified Fraud Examiners:

1. A Certified Fraud Examiner shall, at all times, demonstrate a commitment to professionalism and diligence in the performance of his or her duties.
2. A Certified Fraud Examiner shall not engage in any illegal or unethical conduct or any activity which would constitute a conflict of interest.
3. A Certified Fraud Examiner shall, at all times, exhibit the highest level of integrity in the performance of all professional assignments, and will accept only assignments for which there is a reasonable expectation that the assignment will be completed with professional competence.

4. A Certified Fraud Examiner will comply with lawful orders of the courts, and will testify to matters truthfully and without bias or prejudice.
5. A Certified Fraud Examiner, in conducting examinations, will obtain evidence or other documentation to establish a reasonable basis for any opinion rendered. No opinion shall be expressed regarding the guilt or innocence of any person or party.
6. A Certified Fraud Examiner shall not reveal any confidential information obtained during a professional engagement without proper authorization.
7. A Certified Fraud Examiner shall reveal all material matters discovered during an examination, which, if omitted, could cause a disorder.
8. A Certified Fraud Examiner shall continually strive to increase the competence and effectiveness of professional services performed under his or her direction.

Fraud is a deceptive action intended for personal or financial gain and a certified fraud examiner is a highly qualified professional who investigates cases of criminal and civil fraud. Fraud comes in all forms, such as embezzlement, payroll frauds, skimming, and expense report frauds. The majority of entities, from small businesses to large corporations have dealt with fraud in some way, shape, or form, which decreases gross revenue every year. A certified fraud examiner uses his or her knowledge of multifaceted financial transactions with their understanding of law, techniques, and ways to resolve fraud allegations. He or she has a solid understanding of how and why fraud occurs.

A certified fraud examiner plays three essential roles:

- Identifying evidence of fraud.
- Conducting interviews and writing reports, and
- Proactively evaluating the fraud risk of a business or organisation.

He or she identifies and gathers the evidence of fraud incidences to form a case, such as billing trends, financial relationships, and financial data. He/She also interviews witnesses and documents statements to include in the report. A certified fraud examiner often testifies his or her findings in cases of fraud allegations to resolve the issues. He/She commonly works with attorneys and law enforcement officers and assists in the arrest of individuals charged with fraud. Many certified fraud examiners help organisation's fraud detection and prevention efforts.

A certified fraud examiner may design, apply, and maintain fraud detection procedures and tools. Some also train others in fraud detection and prevention methods.

Professional Opportunities

17.5

Growing cyber-crimes, failure of regulators to track the security scams, series of cooperative banks bursting all are pinpointing the need for forensic accounting, irrespective of whether we understand the need or not.

Forensic accounting seeks to uncover the what, why, and how behind the computation and reporting of figures. The aim is to ascertain or confirm the substance of those purported transactions.

In the Indian context, Forensic Accountants are the most required in the wake of the growing fraud. The law enforcement officers are the experts in analysing fingerprints and the optics but what about the digital evidence analysis.

Why there is a need for Forensic Accountants?

Forensic Accounting is the specialty practice area that describes engagements that result from actual or anticipated frauds, disputes, or litigations. Forensic Accounting, Fraud Detection & Prevention specialization is in increasing demand considering increasing incidents of cyber-crimes and frauds. It is the practice of utilizing accounting, auditing, CAATs/ Data Mining Tools, and investigative skills to detect frauds/ mistakes. The Government bodies, PSUs, in the insurance sector, Banks and, and Investigating agencies as well as many medium-sized and boutique firms have specialist forensic accounting departments engaging Forensic Auditors.

Very few know about it – Maurice E. Peloubet who coined the term Forensic Accountant in 1946 said that the preparation of financial statements has some but not all of the characteristics of forensic accounting. This statement is enough for the chartered accountants in India to foray into this field. It is s a new child on the block. Central Investigating Agencies like CBI do the forensic accounting work.

The growing number of regulators, the administrative agencies will demand the services like forensic reviews. Cost Accountants are going to find themselves more involved in what is essentially a type of forensic practice. The changing nature of the Accounting and Auditing & assurance standards also confirms this.

Nearly 40 percent of the top 100 American accounting firms are expanding their forensics and fraud services, according to Accounting Today. If this data is of some sense to the Indian scenario, then the day is not far away when forensic practice will contribute to the total revenue of the Indian CMA firm.

According to the '2018 Report to the nation' by the Association of Certified Fraud Examiners (ACFE), there were 2690 cases of occupational fraud from 125 countries printing into loss of more than $7 billion which causes a huge demand for those who can identify and put-up relevant control to prevent such mishap. Out of these 72 cases were from India. Against a backdrop of tough economic conditions and growing corporate governance, demand for forensic accountants is increasing. Practitioners believe that the demand for the services of forensic accountants is growing because of the tightening economic conditions and the increasing scrutiny of how companies are governed.

In such circumstances, there is heightened sensitivity to fraud, and that translates into more efforts to detect and prevent it, as well as to take legal action against the wrongdoers.

Nothing is surprising too that, as this the 'Forensic Audit' has become so familiar these days, and special credit for this goes to Mr. Vijay Mallya and Mr. Nirav Modi and a huge pile of NPA's build-up by state-owned banks.

Pre-requisite of a skilful Forensic Accountant:

(a) Dave Cotton, a qualified CFE has greatly defined the attitude the person should maintain while investigating Fraud and Forensic Cases. He said: 'Many fraud perpetrators aren't as clever at concealing fraud as most people probably think. If CFEs simply remain alert and maintain a high degree of professional skepticism many potential frauds are easy to find'.

(b) A good Forensic Auditor requires immense knowledge of the finance aspects along with a good understanding of internal financial controls as identification of weak control can help to easily catch out the areas where fraud can be carried out.

Professional Qualifications that can give you an extra edge: The Institute of Cost Accountants of India, Kolkata conducting Advanced Diploma in Forensic Audit which gives some insights on the subject and helps to improve the skills and knowledge in Forensic Audit.

Sum Up:

Forensic Audit is a much-required tool in the recent era of Frauds & Misappropriations

"If you see a fraud and do not say fraud, then you are a fraud" … Naasim Nicholas Taleb

The relevance of the concept has been highlighted- especially in the emerging scenario of continuous development in the fields of accounting and auditing. The article also touches upon the various inter-related concepts and the vital areas where the technique of Forensic Auditing can be best used in detecting the misappropriations and manipulations in the financial as well as operational matters.

The manipulations and misappropriations in the corporate world relate back to September, 1720 when after the War of Spanish Succession, the Great Britain signed the Treaty of Utrecht, 1713 with Spain, ostensibly allowing it to trade in the seas near South America. In fact, barely any trade took place as Spain renounced the treaty; however, this was concealed on the Great Britain stock market. A speculative bubble saw the share price reach over £1000 in August 1720, but then crash in September. A Parliamentary inquiry revealed fraud among members of the government, including the Tory Chancellor of the Exchequer- John Aislabie, who was sent to prison and since then there has been a steep rise in such manipulations being continuously occurring all over the world, such as Quintex-Real Estate (1989); Poly Peck-Electronics, Food, Textiles (1990); Bre-X-Mining (1997); Equitable Life Assurance Society-Insurance (2000); WorldCom-Telecommunication (2001); Enron-Energy (2001); Arthur Anderson-Accounting (2002); Parmalat-Food (2003); Refco-Brokering (2005) and of course the securities scam by Harshad Mehta and Ketan Parekh, C.R. Bhansali, Home Trade fraud, M/s Satyam Computer Services Ltd and many more. Some of the Companies which were in news in recent past for the wrong reasons:

1. Vakrangee – No one knows what's wrong with the Company, but still the stock prices kept on falling.
2. Manpasand – Alleged Tax credit claim fraud (Fake invoices exchanged in grey market).
3. LEEL – It is alleged that Promoters just took out the money after selling a business unit.
4. Gitanjali – Fake letter of credit.
5. Eros, Cox and kings – It was alleged that Despite having cash, company defaulted on NCD.

6. DHFL – It is alleged that borrowed funds were used to lend to shell companies owned by operator.
7. IL&FS– Huge bonuses and dividend pay-outs to promoters were alleged.
8. Yes Bank – Alleged Non-disclosure of provisions is been the issue and power of cantered in the hand of one man knew and he was asked by regulators to leave.
9. HEG– A 20 million USD bonus was given to the CEO when shareholders lost more than 80% of value.
10. CG Power – It is alleged that billion dollars taken out via transactions.
11. TATA Sons- The Board aligned to the majority shareholder, gave Cyrus Mistry a glowing performance review only to sack him a few months later.
12. Infosys– The Board first played supplicant to Chief Executive Officer Vishal Sikka, then to former promoter NR Narayan Murthy. Investors paid the price for unstable leadership, and even today, investigations into acquisitions have not been shared with all the stakeholders.
13. Axis Bank– The Board seemed unquestioning of Managing Director and Chief Executive Officer Shikha Sharma, but the regulator wanted her go.
14. ICICI Bank– The Board appeared like a deer in the headlights, dazed by the celebrity of MD & CEO Chanda Kochhar, allowing her continued presence in the company, even as she was being investigated for alleged nepotism.
15. Fortis– Promoters held sway, the board turned a blind eye to many suspicious transactions, and finally shareholders booted them out.

Constituents of Forensic Audits:

1. Assessment of fraud risk factors and evaluating internal controls and standards.
2. Comparison and contrast of various fraud schemes to devise the appropriate internal controls.
3. Developing off-setting internal controls that would limit or prevent these fraud schemes.
4. Using data analysis techniques to identify high-risk transactions for further review and investigation.
5. Evaluating internal controls and identifying ways to plan audits to take advantage of available information systems resources.
6. Evaluating financial and program risk for potential fraud.
7. Applying various evidence-gathering techniques used to detect fraud.
8. Justifying the auditor's conclusion of fraud by providing the evidence needed to support legal and investigative staff.
9. Documenting the evidence and data-gathering process.
10. Sharing the findings with the agency and advise them on how to avoid the fraud in the future.

In the present scenario of revival of corporate law and norms being made stringent, there is an ample space for the overall recognition of such an important technique for identifying frauds. The technique altogether different from the traditional auditing approach has also got its significance where the concept of due diligence has to be applied. Forensic Auditing not only identifies the factors/ reasons adversely affecting the trust in mechanism of trade, finance and investment but also helps in recognizing the destabilizing effect on commercial institutions and corporate houses directly affecting the national progress and putting strain on national resources.

Solved Cases

Case Study: 1

Harshad Mehta and the Stock Market Scam

Who is this Stockbroker from Gujarat?

What happened: During the early 1990s he started facilitating transactions of ready-forward deals among the Indian banks, acting as an intermediary. In this process, he used to raise funds from the banks and subsequently illegally invest the same in the stocks listed on the Bombay Stock Exchange to inflate the stock prices artificially. Mehta again raised a furore on 16 June 1993 when he made a public announcement that he had paid Rupees 1 Crore to the then Congress President and Prime Minister as a donation to the party, for getting him off the case.

How did this happen: Mehta siphoned off around ₹1,000 crore from the banking system to buy stocks on the Bombay Stock Exchange. As he pumped in money, the markets continued to achieve new highs. Retail investors took cues from what Mehta was buying and followed in the footsteps of the 'Big Bull'.

In the period between April 1991 and April 1992, the Sensex went into a frenzy and returned 274 percent, moving from 1,194 points to 4,467. That is the highest annual return for the index.

He also promised the banks higher rates of interest, while asking them to transfer the money into his account, under the guise of buying securities for them from other banks. At that time, a bank had to go through a broker to buy securities and forward bonds from other banks. Mehta used this money temporarily in his account to buy shares, thus hiking up the demand for certain shares (of well-established companies like Associated Cement Companies Limited- ACC, Sterlite Industries, and Videocon) dramatically, selling them off, passing on a part of the proceeds to the bank and keeping the rest for himself. This resulted in stocks like ACC (which was trading in 1991 for ₹ 200/ share) to nearly ₹ 9,000 in just 3 months.

The scam came to light when the State Bank of India reported a shortfall in government securities. That led to an investigation that later showed that Mehta had manipulated around ₹ 3,500 crore in the system. On August 6, 1992, after the scam was exposed, the markets crashed by 72 percent leading to one of the biggest falls and a bearish phase that lasted for two years.

On 23 April 1992, journalist Sucheta Dalal exposed Mehta's illegal methods in a column in The Times of India. Mehta was dipping illegally into the banking system to finance his buying.

Exercise

A. Theoretical Questions

Multiple Choice Questions

1. Forensic Accounting is defined as:

   (a) The practice of applying defined financial ratios to investigate a company's financial health.

   (b) The use of law enforcement to subpoena financial records to determine unlawful actions.

   (c) The application of investigative and analytical skills to resolve financial issues in a manner that meets standards required by courts of law.

   (d) The investigatory arm of the Securities and Exchange Commission.

2. If your actions are the result of misleading, intentional actions or inaction (including misleading statements and the omission of relevant information to gain an advantage, then you have committed:

   (a) Perjury.

   (b) Contempt.

   (c) Treason.

   (d) Fraud.

3. When the auditor tests the documents by keeping them side by side then it is known as _____.

   (a) Test of impossibility.

   (b) Test of absurdity.

   (c) Juxtaposition test.

   (d) None of the above.

4. As per the study of ACFE, the following category of individuals commit the highest frauds (in monetary terms)_____.

   (a) Low-level management.

   (b) Mid-level management.

   (c) Senior level management.

   (d) All of the above.

5. _____ are the elements of fraud.

   (a) The individual must know that the statement is untrue.

   (b) There is an intent to deceive the victim.

   (c) The victim relied on the statement & The victim is injured financially or otherwise.

   (d) All of the above.

6. A type of fraud where forged emails, forged websites are used to defraud the user is known as _____.
   (a) E-frauds.
   (b) Forgery.
   (c) Phishing.
   (d) None of the above.

7. _____ happens when the fraudster avails multiple loans for the same property simultaneously for a total amount over the actual value of the property.
   (a) Phishing.
   (b) Window dressing.
   (c) Shot gunning.
   (d) Skimming.

8. Pressure, opportunity & _____ are the aspects of a fraud triangle.
   (a) Rationalization.
   (b) Creation.
   (c) Commitment.
   (d) None of the above.

9. A _____ is termed as an indication of a danger or a warning signal.
   (a) Red flag.
   (b) Green flag.
   (c) Amber flag.
   (d) White flag.

10. A _____ is a flag that denotes a "too good to be true scenario".
    (a) Red flag.
    (b) Green flag.
    (c) Amber flag.
    (d) White flag.

11. Significant increase in working capital borrowing as a percentage of turnover is a_____.
    (a) Red flag.
    (b) Green flag.
    (c) Amber flag.
    (d) White flag.

12. A case where an employee doesn't take travel advance but always pays from his pocket is a _____.
    (a) Red flag.
    (b) Green flag.
    (c) Amber flag.
    (d) White flag.

13. Analysing non-verbal cues is important for a forensic auditor while _____.
    (a) Interviewing a suspect.
    (b) Interrogating a suspect.
    (c) (a) & (b) both.
    (d) None of the above.

14. A model categorizing known frauds which lists about 49 different individual fraud schemes grouped by categories and subcategories is known as _____.
    (a) Fraud triangle.
    (b) Fraud square.
    (c) Fraud model.
    (d) Fraud tree.

15. When the fraudster can give a personal justification for fraudulent actions, it is known as _____.
    (a) Pressure.
    (b) Opportunity.
    (c) Rationalization.
    (d) All of the above.

16. Various frauds in the banking sector are:
    (a) Appraisal fraud.
    (b) Mortgage fraud.
    (c) Shot gunning.
    (d) All of the above.

17. Fraudsters may alter cheques to change the name or the amount on the face of cheques. This is called _____.
    (a) Phishing.
    (b) Forgery.

(c) Disbursement fraud.

(d) Skimming.

18. Ratio analysis is one of the key aspects that a forensic auditor has to look _____ at.

(a) Correct.

(b) Incorrect.

(c) Partially Correct.

(d) Cannot be determined.

19. The principle of 3D vision includes _____.

(a) Time dimension analysis.

(b) Space dimension analysis.

(c) Both (a) & (b).

(d) None of the above.

20. "Fraud is a deliberate act of omission or commission by any person, carried out in the course of a banking transaction or the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank" is a definition given by:

(a) SEBI.

(b) RBI.

(c) ICAI.

(d) ACFE.

21. Concept of Red Flag pertains to Which Audit?

(a) Productivity Audit

(b) Energy Audit

(c) Inventory Audit

(d) Forensic Audit

22. Which audit has its basic object to uncover fraud?

(a) Financial Audit

(b) Internal Audit

(c) Cost Audit

(d) Forensic Audit

23. Pressure, motivation and opportunity are part of

(a) Green Flag

(b) Blue Flag

(c) White Flag

(d) Fraud Triangle

24. Which Section of Companies Act,2013 provide Definion of the Term Fraud?

(a) 445

(b) 446

(c) 447

(d) 448

25. Which Section of Companies Act,2013 casts an obligation upon the Auditors of the Company to report fraud to the Central Government?

(a) 143(11)

(b) 143(12)

(c) 143(13)

(d) 143(14)

Essay Type Questions

1. Write a note explaining the Meaning and Definition of Fraud under the Companies Act, 2013 as well as the Criminal Procedure Code, 1973.
2. What do you mean by Forensic Audit? Discuss its need and significance in detail.
3. Write down the similarities and differences between Audit and Forensic Audit.
4. Discuss the elements of Fraud and Civil, Criminal Remedies available against it.
5. Discuss the fundamentals of Forensic Audit.
6. What is the contemporary scenario of Corporate Fraud in India and How Forensic Audit is significant in preventing the same?
7. What are the various kinds of Fraud? Discuss.
8. What are the different methods of Investigation in Forensic Audit?
9. What are Red Flags and Green Flags? Discuss.
10. Write a Note on Field Investigations.

Answer:

⊙ Multiple Choice Questions (MCQ)

1.	(c) The application of investigative and analytical skills to resolve financial issues in a manner that meets standards required by courts of law.
2.	(d) Fraud.
3.	(c) Juxtaposition test.
4.	(c) Senior level management.
5.	(d) All of the above.
6.	(c) Phishing.
7.	(c) Shot gunning.
8.	(a) Rationalization.
9.	(a) Red flag.
10.	(b) Green flag.
11.	(a) Red flag.
12.	(b) Green flag.
13.	(c) (a) & (b) both.
14.	(d) Fraud tree.
15.	(c) Rationalization.
16.	(d) All of the above.
17.	(b) Forgery.
18.	(a) Correct.
19.	(c) Both (a) & (b).
20.	(b) RBI.
21.	(d) Forensic Audit
22.	(d) Forensic Audit
23.	(d) Fraud Triangle
24.	(c) 447
25.	(b) 143(12)