STUDY ON FORENSIC ACCOUNTING AND FRAUD DETECTION

The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

DISCLAIMER

The views expressed in this material are those of author(s). The Institute of Chartered Accountants of India (ICAI) may not necessarily subscribe to the views expressed by the author(s).

The information in this material has been contributed by various authors based on their expertise and research. While every effort have been made to keep the information cited in this material error free, the Institute or its officers do not take the responsibility for any typographical or clerical error which may have crept in while compiling the information provided in this material. There are no warranties/claims for ready use of this material as this material is for educational purpose. The information provided in this material are subject to changes in technology, business and regulatory environment. Hence, members are advised to apply this using professional judgement. Please visit CIT portal for the latest updates. All copyrights are acknowledged. Use of specific hardware/software in the material is not an endorsement by ICAI.

Revised Edition	:	February, 2016
Reprint	:	September, 2017
Committee/Department	:	Committee on Information Technology
Email	:	cit@icai.in
Website	:	www.icai.org/http://cit.icai.org
Price	:	₹ 100/-
ISBN No	:	978-81-8441-822-4
Published by	:	The Publication Department on behalf of the Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi-110 002.
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra - 282 003. September/2016/P2012(Reprint)

Foreword

Specialization in the areas of *Forensic Accounting and Fraud Detection* is more in demand in view of increased incidents of frauds and cyber-crimes. Forensic accountants with their core understanding of accounting, finance and laws with added knowledge of investigative techniques will be able to determine whether an activity is illegal or not. Forensic Accounting and Fraud Detection (FAFD) involves practice of utilizing accounting, auditing, CAATs/ Data Mining Tools and investigative skills to detect frauds/ mistakes. All Government bodies, PSUs, Insurance sector, Banks, Investigating agencies as well as many medium–sized and boutique firms also have specialist forensic accounting departments engaging Forensic Auditors. Forensic accountants usually investigate and analyze financial evidence, develop computerized applications to assist in the presentation and analysis of the evidence presented, communicate their findings in the form of various reports and assist in the legal proceedings in court as an expert witness.

In the wake of recent financial and cyber frauds and need for expertise in this newer area, the Committee on Information Technology (CIT) of the Institute of Chartered Accountants of India (ICAI) has identified Forensic Audit, Fraud Detection & Prevention as one of the niche area and has started conduct of Certificate Course on Forensic Accounting and Fraud Detection.

The Certificate Course on Forensic Accounting and Fraud Detection of ICAI aims to develop such investigative skills that are required to uncover corporate/ business frauds, measure resultant damage, provide litigation support/ outside counsel by applying accounting, auditing principles for the detection of frauds.

This background material of the Certificate Course contains various practical aspects, new technologies and case studies related to Forensic Accounting and Fraud Detection which together will make it a great learning guide and assist the members in understanding the nuances of this complex subject thoroughly. I appreciate the efforts put in by CA. Atul Kumar Gupta, Chairman, CA. Jay Chhaira, Vice-Chairman, other committee members, faculties and officials of CIT for bringing out this background material.

I am sure that it will be a useful learning material and will fulfill the objectives for which it has been developed.

Wishing you all the very best in this emerging professional opportunity.

Best wishes,

Place: New Delhi
Date: 21st September 2017

CA. Nilesh Shivji Vikamsey
President, ICAI

Preface

Recently, Forensic Accounting (FA) has come into limelight due to rapid increase in financial frauds and white-collar crimes. The integration of accounting, auditing and investigative skills creates the specialty, known as FA. 'Forensic' means "suitable for use in a court of law," and it is to that standard and potential outcome that forensic accountants generally have to work. FA uses accounting, auditing, and investigative skills to conduct investigations, and thefts and frauds cases. No doubt, FA is listed among the top-20 careers of the future. The job of forensic accountants is to catch the perpetrators of the financial theft and fraud occurring throughout the World every year. This includes tracing money laundering and identity theft activities, as well as, tax evasions.

Forensic accountants will be in high demand because of an increase in employee and management fraud, theft, embezzlement and other financial crimes. Growth is also fueled by high-visibility corporate scandals. The Bureau of Labor Statistics (BLS) USA has predicted 13% job growth for accountants and auditors by 2022. The growth of all forensic accounting jobs should correspond with this rate, if not exceed it, due to increasing financial regulations, with some estimates predicting a 20% growth in demand for investigative auditors.

This Course is a blend of theoretical and practical training and is intended to equip the participants with concepts in Forensic Accounting which aims at sensitizing Fraud Investigators, Auditors, Security Professionals, and IT executives about the risks and mitigation strategies for an effective business environment, update members on the developments taking place in the exciting world of forensic investigation related to finance and Information Technology sector. It provides an incisive analysis of how fraud occurs within an organization and explains the latest techniques for fighting it.

This background material is prepared so as to cover all major aspects applicable to Forensic Accounting and is intended to provide an understanding about the current state of Frauds, Technologies involved and their characteristics and give a well-knitted overview & assessment approach along with that of the prevailing cyber laws/ IT Act.

I would like to express my gratitude to CA. Nilesh Shivji Vikamsey, President ICAI and CA. Naveen N. D. Gupta, Vice President for their continuous support and

encouragement to the initiatives of the Committee. I must also thank my colleagues from the Council at the Committee on Information Technology for providing their invaluable guidance as also their dedication and support to various initiatives of the Committee.

I would also like to extend my sincere thanks and appreciation to CA Sailesh Cousik, CA Durgesh Pandey, CA Abhijit Sanzgiri, CA Yogesh Palekar, CA Shanobar Murali, CA Chetan Dalal, CA Mahesh Bhatki, CA Anand Jangid, CA M. S. Mehta, Mr. Alok Gupta, CA. Rajiv Gupta, Mr. Prashant Mali, CA. Ravi Suriyanarayanan, CA T.V.Balasubramaniam, and Dr. Triveni Singh, who contributed the technical material for this publication brought out by the Committee on Information Technology. I really appreciate their sincere efforts and dedication towards the work for the Committee.

I wish to express my thanks to Committee Secretariat in giving final shape to the publication.

I take pleasure in inviting you all to this Course on Forensic Accounting and Fraud Detection and I am sure that all the participants will immensely benefit from this Course.

CA Atul Kumar Gupta
Chairman
Committee on Information Technology

Contents

Chapter 1
Introduction to Forensic Accounting

Forensic

The word forensic comes from the Latin word forēnsis, meaning "of or before the forum."

Means –

- Relating to, used in, or appropriate for courts of law or for public discussion or argumentation.
- Relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law

Forensic Accounting

The integration of accounting, auditing and investigative skills yields the specialty known as Forensic Accounting. It is the study and interpretation of accounting evidence. It is the application of accounting methods to the tracking and collection of forensic evidence, usually for investigation and prosecution of criminal acts such as embezzlement or fraud.

Forensic Investigation

Also known as forensic audit is the examination of documents and the interviewing of people to extract evidence. Forensic Accounting examines individual or company financial records as an investigative measure that attempts to derive evidence suitable for use in litigation.

Forensic Accounting can sometimes be referred to as Forensic Auditing.

Purpose can be:

- A forensic audit can be conducted in order to prosecute a party for fraud, embezzlement or other financial claims
- In addition, an audit may be conducted to determine negligence

Fraud auditing

In a fraud audit one searches for the point where the numbers and/or financial statements do not mesh. It is a meticulous review of financial documents conducted when fraud is suspected. Some entities do them as a precaution to prevent fraud from happening and to catch it before the loss magnifies.

A Fraud Audit however is not an Investigation. *Fraud auditing is used to identify fraudulent transactions, not to figure out how they were created*. The auditor simply traces every

transaction performed by the company, looking for the one that is fraudulent, if any. A regular auditor simply checks the numbers for accuracy.

Fraud auditors often go outside the books of accounts to find fraudulent transactions. This may include reviewing receipts, not only from the company, but from customers as well. Any inconsistencies in these numbers could help uncover an act of fraud. These auditors also interview employees, customers and sometimes clients to find out if a fraud has taken place.

How is a forensic accounting analysis different from an audit?

The general public believes that a financial auditor would detect a fraud if one were being perpetrated during the financial auditor's audit. The truth, however, is that the procedures for financial audits are designed to detect material misstatements, not immaterial frauds. While it is true that many of the financial statements and frauds could have, perhaps should have, been detected by financial auditors, the vast majority of frauds could not be detected with the use of financial audits. Reasons include the dependence of financial auditors on a sample and the auditors' reliance on examining the audit trail versus examining the events and activities behind the documents. The latter is simply resource prohibitive in terms of costs and time.

There are some basic differences today between the procedures of forensic auditors and those of financial auditors. In comparison, forensic accounting and audit differ in specific ways, as shown below:

Forensic Accounting

- In response to an event
- Financial investigation
- Findings used as evidence in court or to resolve disputes

Audit

- Mandatory
- Measures compliance with reporting standards
- Obtain reasonable assurance that financial statements are free of material misstatement

In practice, there are differences in mindset between forensic accounting and audit:

- "Investigative mentality" vs. "professional skepticism". A forensic accountant will often require more extensive corroboration.
- A forensic accountant may focus more on seemingly immaterial transactions.

A forensic accountant will often look for indications of fraud that are not subject to the scope of a financial statement audit.

Sr. No.	Particulars	Other Audits	Forensic Audit
1.	Objectives	Express an opinion as to 'True & Fair presentation	Whether fraud has taken place in books
2.	Techniques	Substantive & Compliance. Sample based	Investigative, substantive or in depth checking
3.	Period	Normally for a particular accounting period	No such limitations.
4.	Verification of stock, estimation realizable value of assets, provisions, liability etc.	Relies on the Management certificate / Management Representation	Independent verification of suspected / selected items where misappropriation is suspected
5.	Off balance sheet items (like contracts etc.)	Used to vouch the arithmetic accuracy & compliance with procedures.	Regulatory& propriety of these transactions / contracts are examined.
6.	Adverse findings if any	Negative opinion or qualified opinion expressed with/without quantification	Legal determination of fraud impact and identification of perpetrators depending on scope. .

What is Fraud?

Fraud is a type of criminal activity, defined as:

'abuse of position, or false representation, or prejudicing someone's rights for personal gain'.

Put simply, fraud is an act of deception intended for personal gain or to cause a loss to another party.

The general criminal offence of fraud can include:

- deception whereby someone knowingly makes false representation
- or they fail to disclose information
- or they abuse a position.

Apart from the general meaning let us study some notable definitions of Fraud as per various statutes and standards. Although definitions vary, most are based around the general theme mentioned above

The **Companies Act, 2013** defines Fraud in relation to affairs of a company or anybody corporate, to include,

(a) any act

(b) omission,

(c) concealment of any fact

(d) abuse of position committed by any person or any other person with the connivance in any manner

- ❖ with intent to deceive
- ❖ 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;

- *"wrongful gain"* means the gain by unlawful means of property to which the person gaining is not legally entitled
- *"wrongful loss"* means the loss by unlawful means of property to which the person losing is legally entitled

Fraud is also defined in **Para 11(a) of SA 240** issued by the Institute of Chartered Accountants of India –"Auditors Responsibilities relating to Fraud in Audit of Financial Statements" as

'An intentional act by one or more individuals among

- Management
- those charged with governance
- employees or
- or third parties,

Involving use of deception to obtain an unjust or an illegal advantage."

Similarly **Standards on Internal Audit** i.e. **SIA 11** – "Consideration of Fraud in an Internal Audit define Fraud as

"An intentional act by one or more individuals among management, those charged with governance or third parties involving the use of deception to obtains unjust or illegal

advantage. A Fraud could take form of misstatement of an information (Financial or otherwise) or mis-appropriation of assets of that entity"

Another notable definition of Fraud is the one of Indian Contract Act. According to **Section 17** of the **Indian Contract Act, 1872**

'Fraud' **means and includes** any of the following acts committed by

- a party to a contract or
- with his connivance,
- or by his agent,

With an intent to

- Deceive another party thereto or
- His agent or
- To induce him to enter into the contract

1. The suggestion, as a fact, of that which is not true, by one who does not believe it to be true
2. The active concealment of a fact by one having knowledge or belief of the fact
3. A promise made without any intention of performing it
4. Any other act fitted to deceive
5. Any such act or omission as the law specially declares to be fraudulent

Explanation:

Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak, or unless his silence, is in itself, equivalent to speech.

This can be illustrated by way of an example –A sells, by auction, to B, a horse which A knows to be unsound. A says nothing to B about the horse's unsoundness. This is not fraud in A sells, by auction, to B, a horse which A knows to be unsound. A says nothing to B about the horse's unsoundness. This is not fraud in A."

Also Section 25 of IPC defines "Fraudulently" as: A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

The purpose of fraud may be monetary gain or other benefits.

Here is an insight on certain other statutes/standards/circulars/framework principles which have mentions of frauds and have given a framework with regards to their prevention, classification, detection and reporting

Circular No. IRDA/SDD/MISC/CIR/009/01/2013 date 22nd October 2013 issued by **IRDA** has mentions of Fraud in Insurance Sector an act of omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for other related parties.

Circular No. RBI/2014-15/85 by **RBI** dated 1st July 2015 on Fraud Classification and Reporting in Banking Sector – Gives classification of Frauds based on the provisions of the Indian penal code mainly to have uniformity in reporting.

COSO principle 8 – talks of "Consider potential of Fraud". It requires identifications of the opportunities, pressures, incentives, attitudes & rationalizations that may lead stakeholders to act outside the boundaries of ethical conduct & standards of behaviour.

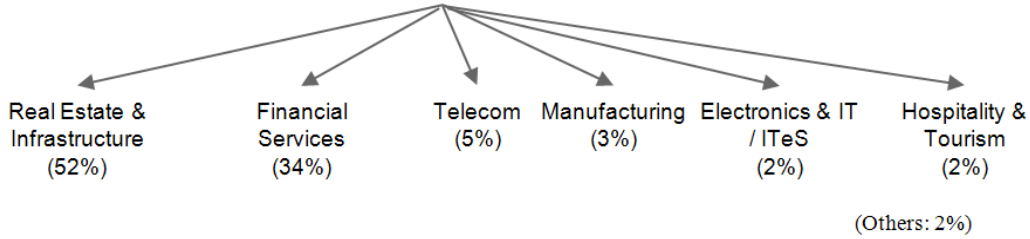
SA 240 This Standard on Auditing (SA) deals with the auditor's responsibilities relating to fraud in an audit of financial statements and expands on how SA 315, "Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment," and SA 330, "The Auditor's Responses to Assessed Risks," are to be applied.

SA 315 requires the auditor to identify and assess the risks of material mis statements whether due to fraud or error in the financial statements.

Chapter 2

Where are the Fraud Vulnerabilities and Why do they Occur

As per a recent study by Assocham and Grant Thornton, the most vulnerable sectors to Fraud in India are:



The increasing adverse effects of Fraud merit it's further study and the first step in that study is understanding as to **'Why do Frauds Happen'** So let us study some of the principles/theories which shall help us understand as to why frauds happen.

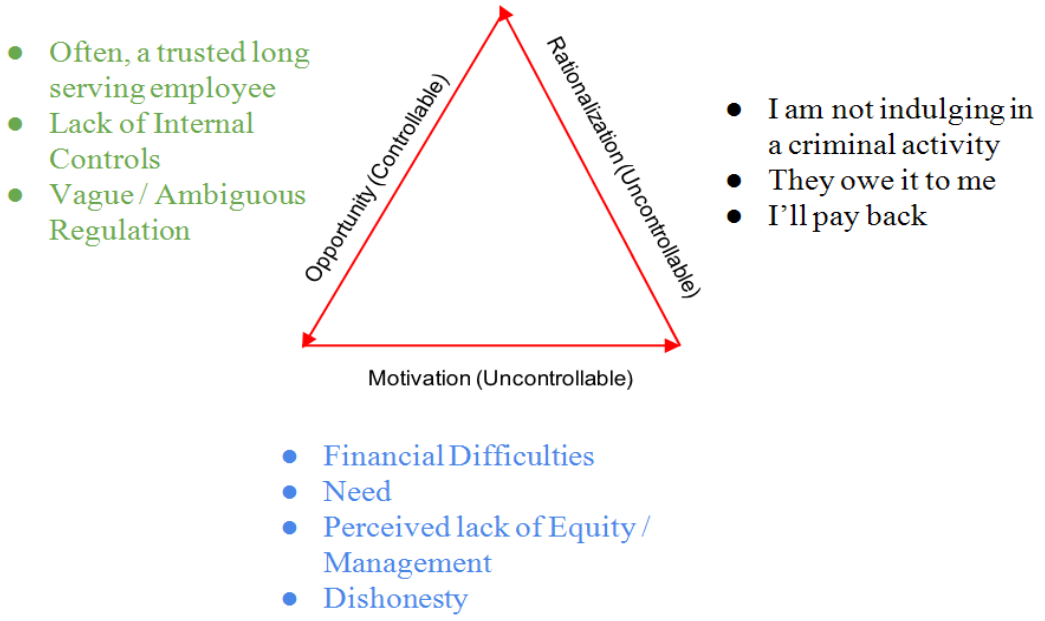
The most basic of all theories is the Fraud Triangle Theory. The other theories are merely extension of Fraud Triangle Theory.

2.1 Fraud Triangle

Donald Cressey, a sociologist and criminologist in the 1940s, was one of the first persons to specialize in the field of understanding fraudsters and why they do what they do. Cressey wrote "Theft of the Nation," a treatise on La Cosa Nostra- a hierarchically structured view of the Organizational Crime and he was widely known for his studies in organized crime. Cressey first gained public recognition in this field while completing his PhD dissertation on embezzlers, at Indiana University. Cressey interviewed nearly 200 incarcerated individuals charged with embezzlement. From his research, Cressey developed "The Fraud Triangle" which was a model he used to explain what caused some people to become fraudsters by analyzing the circumstances in which the subjects of his research were drawn into fraud

The fraud triangle, developed by Donald Cressey, is a model for explaining the factors that cause someone to commit occupational fraud. It consists of three components which, together, lead to fraudulent behavior:

1. Perceived Pressure
2. Perceived opportunity
3. Rationalization



Incentive/ Pressure

Management or other employees may find themselves offered incentives or placed under pressure to commit fraud. When, for example, remuneration or advancement is significantly affected by individual, divisional, or company performance, individuals may have an incentive to manipulate results or to put pressure on others to do so. Pressure may also come from the unrealistic expectations of investors, banks, or other sources of finance. Certain risk factors are usefully considered in the evaluation of whether or not the organization is at a greater or lesser degree of risk, owing to incentives or pressures that could potentially lead to material misstatements.

Determining the presence and degree of these pressures or incentives is part of the auditor's goal in evaluating the risk that misstatements due to fraud may have occurred.

Certain risk factors are usefully considered in the evaluation of whether or not the organization is at a greater or lesser degree of risk, owing to incentives or pressures that could potentially lead to material misstatements.

- Financial stability or profitability is threatened by economic, industry, or entity operating conditions.
- Excessive pressure exists for management to meet debt requirements
- Personal net worth is materially threatened

Attitudes/ rationalization

Some individuals are more prone than others to commit fraud. Other things being equal, the propensity to commit fraud depends on people's ethical values as well as on their personal circumstances. Ethical behavior is motivated both by a person's character and by external factors. External factors may include job insecurity, such as during a downsizing, or a work environment that inspires resentment, such as being passed over for promotion.

Risk factors that fall into this category of rationalization and attitude are typically the least tangible or measurable, and many are by nature difficult for an auditor to observe or otherwise ascertain. Fundamentally, rationalization and attitude are functions of the culture of an organization, the psychology of those who work in it, and the interaction between the two—for example, the level of employee loyalty to the company. The wider business environment must also be considered: hard times in an industry or in the overall economy may make it easier for some individuals to rationalize fraud.

- A history of violations of laws is known
- Little communication and support of the entity's core values is evident.
- Management has a practice of making overly aggressive or unrealistic forecasts.
- Personal financial obligations create pressure to misappropriate assets.
- Adverse relationships between management and employees motivate employees to misappropriate assets.
- Disregard for the need to monitor or reduce risk of misappropriating assets exists.
- There is a disregard for internal controls

Some of the commonly given reasons for committing Fraud –

1. Everyone else is doing it
2. I needed the money
3. I meant no harm and did no harm
4. The organization can afford it
5. I was used and needed revenge
6. What I did was entirely right for someone in my position
7. My employer did not compensate me well enough and hence I took what was due to me
8. Bribery is a norm in this type of business
9. I did it to keep the business afloat
10. It was a loan and I would have repaid it

Opportunities

Circumstances may exist that create opportunities for management or other staff to commit fraud. When such opportunities arise, those who might not otherwise be inclined to behave dishonestly may be tempted to do so. Even individuals under pressure and susceptible to incentives to perpetrate a fraud are not a grave threat to an organization unless an opportunity exists for them to act on their need. An opportunity must exist to commit fraud, and the fraudster must believe the fraud can be committed with impunity.

Opportunities may also be inherent in the nature, size, or structure of the business. Certain types of transactions lend themselves more than others to falsification or manipulation, as do certain kinds of balances or accounts.

- There is a presence of large amounts of cash on hand or inventory items.
- There is an inadequate internal control over assets.
- Inadequate segregation of duties.
- Absence of mandatory job rotation and vacations.

2.2 Fraud Diamond

Wolf and Hermanson (2004) introduced the fraud diamond model where they presented another view of the factors to fraud. The theory adds fourth variable **"Capability"** to the three factor theory of fraud triangle. Wolf and Hermanson believed many frauds would not have occurred without the right person with right capabilities implementing the details of the fraud. They also suggested four observation traits for committing fraud:

- Authoritative position or function within the organization.
- Capacity to understand and exploit accounting systems and internal control
- Confidence that he/she will not be detected, or if caught, he/she will get out ofit easily.
- Capability to deal with the stress created within and otherwise good person• when he or she commits bad act.

The Fraud Diamond theory states that all these 3 ingredients are essential but the critical component in turning the fraud opportunity into reality is "Capability". The fraudster should have the necessary traits and abilities to be the right person to pull it off and also the confidence and ego that he will not be detected or he will be able to talk himself out of trouble if detected.

2.3 Fraud Pentagon

Cressey's classic fraud triangle helps to explain many situations, but today's fraudster is more independent-minded and armed with more information and access than were available to perpetrators in the 1950s. In addition, few would deny there have been significant cultural changes in the past 60 years. The fraud triangle can be expanded further to a Crowe Horwath's Fraud Pentagon, where an employee's competence and arrogance are factored into the 3 conditions generally present when fraud occurs. The two additional aspects in the Fraud Pentagon are:

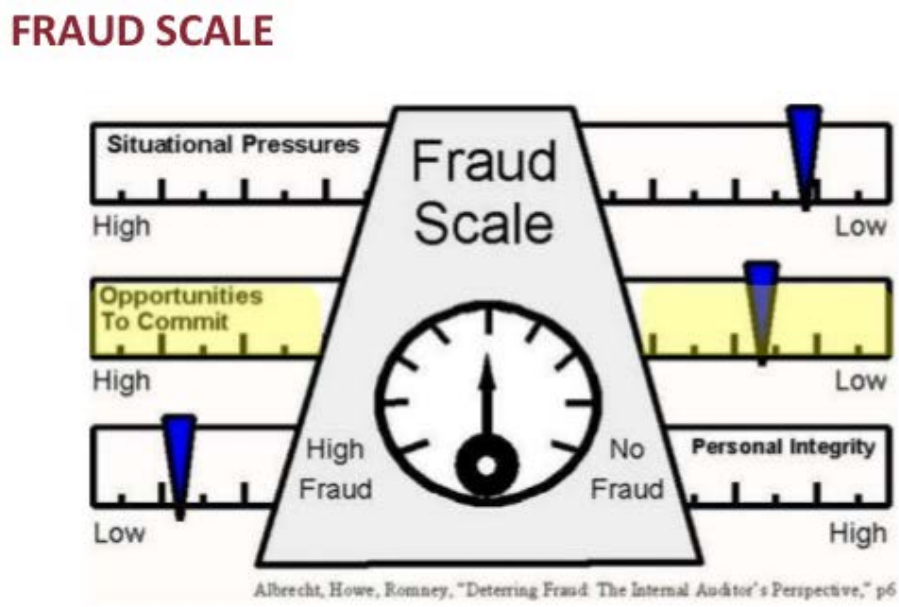
1. **Competence**: It is an extension on the element of opportunity to include an individual's ability to override internal controls and to socially control the situation to his advantage

2. **Arrogance (lack of conscience):** It is an attitude of superiority and entitlement or greed on the part of the perpetrator who believes that company policies and procedures do not apply to him.

2.4 Fraud Scale

This is another theory on Frauds propounded by Steve Albrecht which states -

- Situational pressures, perceived opportunities& personal integrity are the 3 factors that lead to frauds–
- When situational pressures & perceived opportunities are high & personal integrity is low, occupational fraud is much more likely to happen than when the opposite is true.
- It also states that perpetrators hard to profile & fraud difficult to predict.



2.5 Fraud Circle

Another notable theory relating to Fraud is of 'Fraud Circle'. This theory recognizes the fact that fraud is Omni-present everywhere and wherever there will be money there will always be Frauds

2.6 Hollinger Clark Theory

Hollinger and Clark study was based on a total of 12,000 employees of various organizations. They found that nearly 90% engaged in 'work place deviance' which included behavior such as gold bricking, workplace slowdowns, sick time abuses and pilferage. On top of that, an astonishing one third of employees actually had stolen money or merchandise on job. The researchers concluded that the most common reason employees committed fraud had little to do with opportunity, but more with motivation. The more dissatisfied the employee the more likely he or she was to engage in criminal behavior. This is described as employees taking wages in kind.

Hollinger and Clark concluded that everyone had a sense of their own worth, if they believe that they are not being fairly treated or adequately compensated, statistically the organization is at much higher risk of employee related frauds.

Chapter 3
Types of Frauds

Fraud auditing is designed to look for six types of fraud, according to Business Network's "Recognizing Fraud Indicators." These are embezzling, bribes, stealing, extortion, fictitious transactions, kickbacks and conflict of interest. Although not all fraud cases can be easily classified, they will always---at the very least---involve one of these categories. Fraud auditors are trained to look specifically for indicators to any of these fraud types.

If we classify frauds based on industry, Following are the types of frauds:

1. Bank frauds
2. Corporate frauds
3. Insurance frauds
4. Health Care Frauds
5. Cyber frauds
6. Securities frauds
7. Consumer frauds

3.1 Bank Frauds:

The number of bank frauds in India is substantial. It is in increasing with the passage of time in all the major operational areas in banking. There are different areas where fraud may exist, like- Bank-Deposits, Inter-Branch Accounting, Transactions etc.

As a customer you may be seen as a potential target for fraudulent activities. However by arming yourself with information and tools you can protect yourself from becoming a victim of fraud. Do you know the four biggest fraud threats you face?

- Electronic fraud
- Identity theft
- Credit/Debit card fraud
- Cheque fraud.

Credit/Debit card fraud

Credit card and debit card fraud is a crime whereby your credit or debit card can be reproduced in order to use the credit balance to obtain a financial advantage. The creation and/or alteration of a credit/debit card occurs when the information contained on the magnetic

strip is reproduced. This type of crime is known as 'skimming'.

Credit or debit card fraud can also occur when your card is lost or stolen and used by a third party to purchase goods with those cards or to remove cash from the cards.

Credit or debit cards can also be intercepted in transit while being sent to you. Your cards can also be compromised by a dishonest merchant who undertakes unauthorized duplicate transactions on your card.

Cheque Fraud

Cheque fraud is the use of a cheque to get financial advantage by:

- altering the cheque (payee/amount) without authority
- theft of legitimate cheques and then altering them
- duplication or counterfeiting of cheques
- using false invoices to get legitimate cheques
- depositing a cheque into a third party account without authority
- depositing a cheque for payment knowing that insufficient funds are in the account to cover the deposited cheque.

3.2 Corporate Frauds

Corporate Frauds can be defined as 'Activities undertaken by an individual or company that are done in a dishonest and illegal manner and are designed to give an advantage to the perpetrating individual or company' In India, corporate fraud is on a rising trend of45% when leading Indian business declared that fraud e.g. Satyam Computers stunned the national financial world. In 2009 Satyam Founder B. Ramalinga Raju declared he had inflated profit and jacked up the company's Balance Sheet by more than one billion dollars.

In the Corporate environment frauds which are committed by employees of the organization are referred to as Occupational or Employee Frauds.

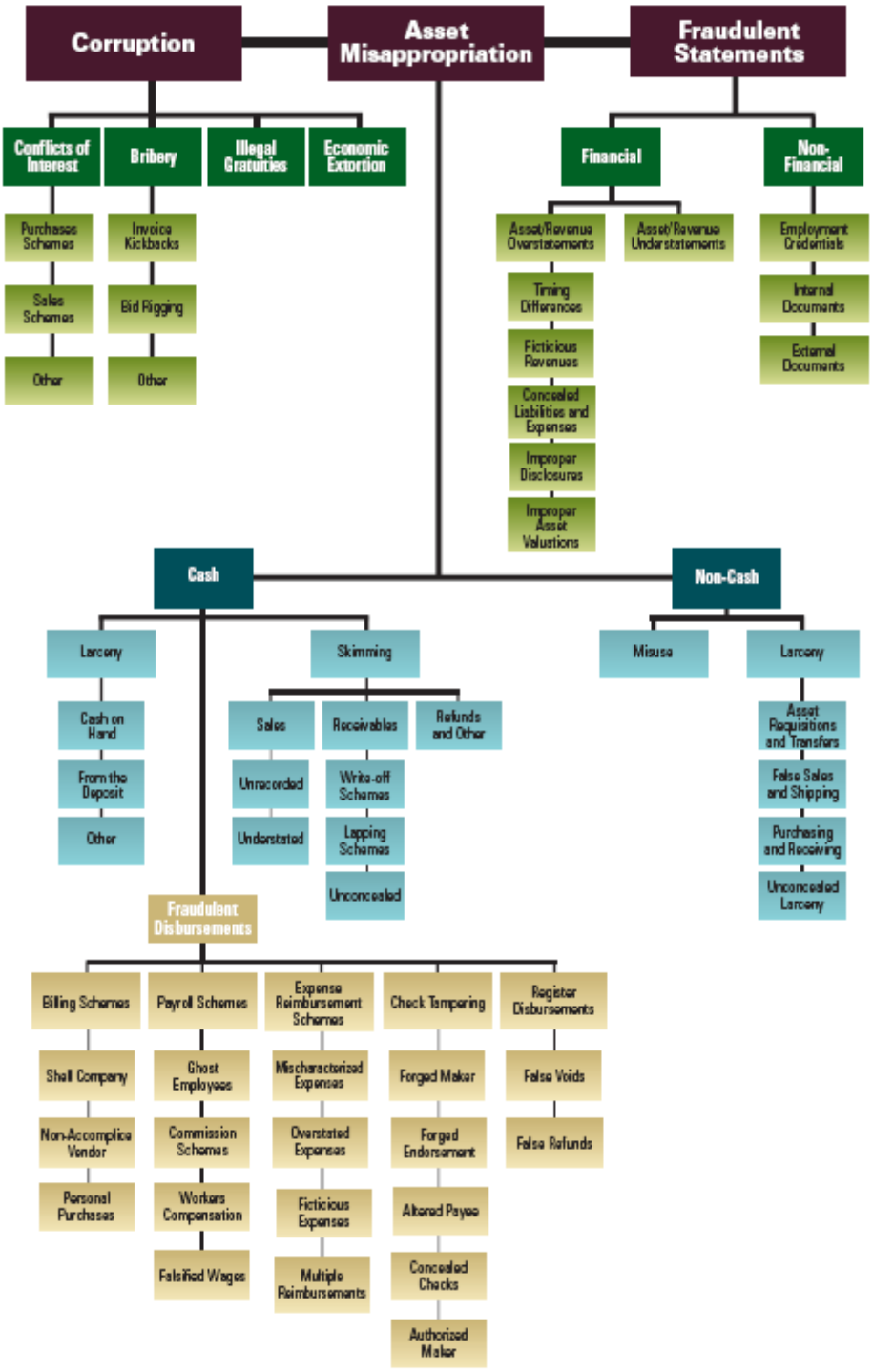
Occupational Fraud is also defined as an employee's misuse or abuse of his position for his own enrichment by intentional misappropriation or misuse of company assets. This may include fraud by an employee, manager or statutory representative.

Occupational Fraud is broadly classified into 3 types

1. Corruption
2. Asset Misappropriation
3. Fraudulent Financial Statements

The FRAUD TREE provides a visual representation of the 3 categories of Occupational Fraud broken down into various sub-categories.

Occupational Fraud and Abuse Classification System



Classification of Occupational in the Fraud Tree is as follows

Financial Statement Frauds: The least common type of fraud amongst the 3 categories of Fraud in terms of occurrence is the financial statement fraud. Although it occurs least frequently, in only 10% of all fraud cases, it is easily the most expensive. The average financial statement fraud cost to a Company is very high. This type of fraud centers on the manipulation of financial statements in order to create financial opportunities for an individual or entity. Stock price, increased year-end bonuses, favorable loan terms, or other indirect benefits are few of the reasons as to why financial statement frauds are committed Financial Statement fraud means manipulation, falsification & alteration of accounting records – (Inventory manipulation, over & under invoicing, Advance billing, Non-impairment of assets, and use of related party transactions not at arm's length pricing)

This manipulation could be done by booking fictitious Income or Advance Booking of Income or non-booking / non-accrual of expenses to increase profits to avail loans / credit or boost share prices or Reduce Income or inflate Expenses to reduce profits with a view to pay lower taxes. Alternatively assets like stock or book debts could be inflated to arrive at an inflated drawing Power to enable more credit to be obtained.

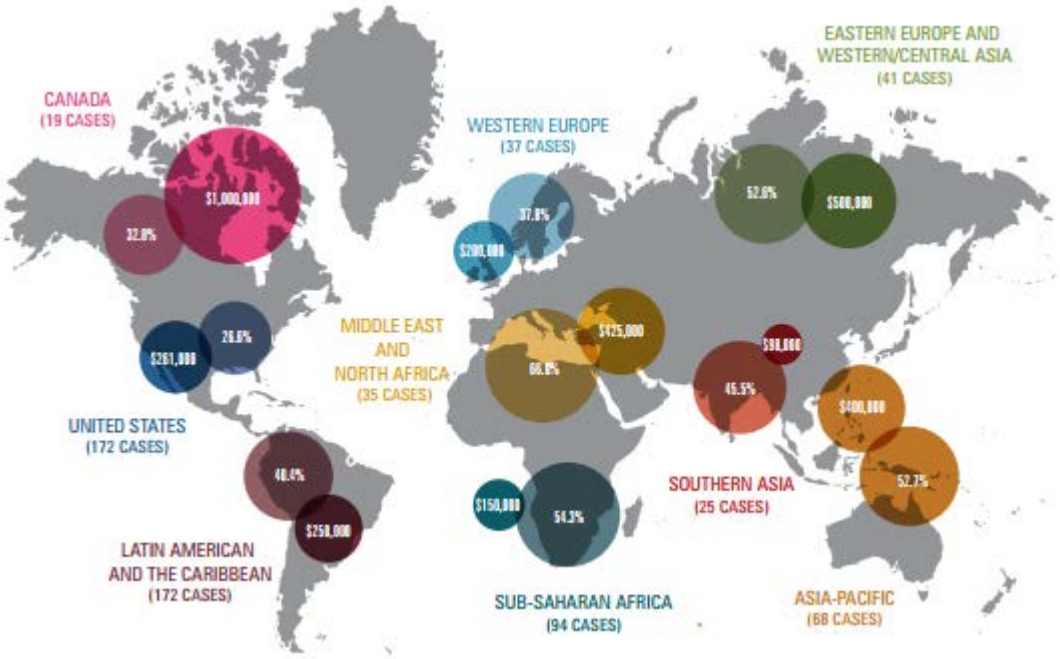
Falsifying documents wholly or in part is termed **Forgery**

The practice of presenting a rosier picture than what is in reality is also termed as **Window Dressing** or **Ever Greening**.

Corruption: The next most frequently occurring fraud scheme is corruption and bribery, which is part of about 30% of all fraud that is uncovered. Bribery and corruption include schemes such as kickbacks, shell company schemes, bribes to influence decision-making, manipulation of contracts, or substitution of inferior goods. The average bribery/corruption scheme is far more costly than asset misappropriation but less costly than Financial Statement Fraud.

In 'Report to the nations on occupational Fraud and Abuse' ACFE identified the breakdown of corruption cases by region, along with the respective median losses of those cases (given in the pictorial format below) TheMiddle East and North Africa had the largest percentage of reported corruption cases This analysis only represents the cases reported to ACFE by the CFEs who investigated those cases, and therefore it does not necessarily reflect overall levels of corruption in each region.

It is also worth noting that Transparency International's 2013 Corruption Perceptions Index found these two regions to have amongst the highest perceived levels of corruption in the world



Asset Misappropriation: This type is the most common, probably because they are the frauds that occur most often and are the easiest schemes to understand. An asset misappropriation might include things like check forgery, theft of money, inventory theft, payroll fraud, or theft of services. Misappropriation happens in over 91% of fraud schemes. This easily makes it the most common fraud, but in terms of losses it is the least expensive per median loss amongst the 3 categories.

3.3 Insurance Frauds

Insurance fraud is any act committed with the intent to obtain a fraudulent outcome from an insurance process. This may occur when a claimant attempts to obtain some benefit or advantage to which they are not otherwise entitled, or when an insurer knowingly denies some benefit that is due. According to the United States Federal Bureau of Investigation the most common schemes include: Premium Diversion, Fee Churning, Asset Diversion, and Workers Compensation Fraud. The perpetrators in these schemes can be both insurance company employees and claimants. False insurance claims are insurance claims filed with the intent to defraud an insurance provider.

Insurance fraud has existed since the beginning of insurance as a commercial enterprise. Fraudulent claims account for a significant portion of all claims received by insurers. Types of insurance fraud are diverse, and occur in all areas of insurance. Insurance crimes also range in severity, from slightly exaggerating claims to deliberately causing accidents or damage. Fraudulent activities affect the lives of innocent people, both directly through accidental or intentional injury or damage, and indirectly as these crimes cause insurance premiums to be

higher. Insurance fraud poses a significant problem and governments and other organizations make efforts to deter such activities.Such instances of Fraud have been occurring both in the life and non-life sector. There are significant opportunities for professionals in the field of forensics and risk management both in the assessment of risk for insurance sector as well as in determining the veracity of the claims.

According to a survey carried out by E&Y "Fraud risk poses a very big challenge for the insurance sector. Business leaders are aware of the need to address this risk, but the lack of a comprehensive and integrated approach to fraud risk management continues to be a concern. The increasing number of frauds and the growing degree of risk necessitates that insurance companies regularly review their policies, build in checks and use new and advanced technology to avoid such issues. However, no system can be foolproof, but a proactive and dynamic approach can make a company ready to counter fraudsters and gain an edge over its competitors."

The key Findings of the survey are still valid today

- There have been increased incidences of fraud over the last one year.
- Fraud risk exposure from claims or surrender is a major concern area for industry players. They have emphasized the need for increased anti-fraud regulations in the area of claims management
- Frauds are driving up overall costs for insurers and premiums for policyholders.
- There is a need for a more robust data analytics tools to effectively detect red flags.
- It's imperative to screen all the key vendors.

3.4 Cyber Frauds

Cyber-crime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cyber-crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber-crimes when the illegal activities are committed through the use of a computer and the Internet.

The increasing penetration of e-commerce into consumer population has made this a swiftly emerging area of practice for forensic accounting professionals

3.5 Securities Frauds

These scams occur because of manipulation of the market by either "insiders" or large players in the stock market who cause stock prices to fluctuate unusually for their own personal gain, either through use of "insider" information or through unfair trading practices. As a result common small investors lose a lot of money as through ignorance they fall into temptation and invest in stocks which they would not have had they had any idea of how the markets were being manipulated.

3.6 Consumer Frauds

Consumer frauds means defrauding consumers of various products and services which do not perform as advertised. These types of schemes take the form of false advertising, unfair terms and service conditions, unfair pricing etc.

Chapter 4
Forensic Accounting: Scope

With India being ranked as the 88th most corrupt nation, the needs for forensic accountants become all the more profound. A Forensic Auditor is often retained to analyze, interpret, summarize and present complex financial and business related issues in a manner which is both understandable and properly supported. Forensic Accountants are trained to look beyond the numbers and deal with the business reality of the situation.

Forensic Auditors can be engaged in public practice or employed by insurance companies, banks, police forces, government agencies and other organizations.

A Forensic Auditor is often involved in the following:

- **Fraud Detection**: Investigating and analyzing financial evidence, detecting financial frauds and tracing misappropriated funds
- **Computer Forensics:**Developing computerized applications to assist in the recovery, analysis and presentation of financial evidence;
- **Fraud Prevention:** Either reviewing internal controls to verify their adequacy or providing consultation in the development and implementation of an internal control framework aligned to an organization's risk profile
- **Providing Expert Testimony**: Assisting in legal proceedings, including testifying in court as an expert witness and preparing visual aids to support trial evidence.

In order to properly perform these services a Forensic Auditor must be familiar with legal concepts and procedures and have expertise in the use of IT tools and techniques that facilitate data recovery and analysis. In addition, a Forensic Auditor must be able to identify substance over form when dealing with an issue.

Fraud Detection

- Review of the factual situation and provision of suggestions regarding possible courses of action.
- Assistance with the protection of assets and preventing recurrence.
- Co-ordination of other experts, including:
    - Private investigators;
    - Forensic document examiners;
    - Consulting engineers.

- Assistance with the recovery of assets by way of tracing misappropriated funds and subsequent civil action or criminal prosecution.

Litigation Support

- Assistance in obtaining documentation necessary to support or refute a claim.
- Review of the relevant documentation to form an initial assessment of the case and identify areas of loss.
- Assistance with Examination for Discovery including the formulation of questions to be asked regarding the financial evidence.
- Attendance at the Examination for Discovery to review the testimony, assist with understanding the financial issues and to formulate additional questions to be asked.
- Review of the opposing expert's damages report and reporting on both the strengths and weaknesses of the positions taken.
- Assistance with settlement discussions and negotiations.
- Attendance at trial to hear the testimony of the opposing expert and to provide assistance with cross-examination.

Forensic Auditors are retained by:

- Lawyers
- Police Forces
- Insurance Companies
- Government Regulatory Bodies and Agencies
- Banks
- Courts and
- Business Community

Forensic Auditors' Services

- Crafting questions to be posed
- Responding to questions posed
- Identifying documents to be requested and/or subpoenaed
- Identifying individuals to be most knowledgeable of facts
- Conducting research relevant to facts of the case
- Identifying and preserving key evidence

- Evaluating produced documentation and information for completeness
- Analyzing produced records and other information for facts
- Identifying alternative means to obtain key facts and information
- Providing questions for deposition and cross examination of fact and expert witnesses

Why are Forensic Auditors required?

They can resolve the matters by combining accounting knowledge & experience with respect to:

- Fraud Prevention
- Fraud Detection
- Internal Controls Implementation and Review
- Compliance and Regulatory Functions
- Evidence Collection and Analysis
- Risk Management
- Court systems
- Filing requirements
- Investigative methodologies
- Assignments with regulatory agencies like SEBI, RBI. EOW etc.
- Professional body to provide expertise and literature in this fast growing field
- Communicating with audiences from attorneys & judges to victims & suspects

The services rendered by the forensic accountants are in great demand in the following areas:

1. Criminal Investigation

Matters relating to financial implications the services of the forensic accountants are availed of. The report of the accountants is considered in preparing and presentation as evidence.

2. Cases relating to professional negligence

Professional negligence cases are taken up by the forensic accountants. Non-conformation to Generally Accepted Accounting Standards (GAAS) or non-compliance to auditing practices or ethical codes of any profession they are needed to measure the loss due to such professional negligence or shortage in services.

3. Arbitration service

Forensic accountants render arbitration and mediation services for the business community.

Their expertise in data collection and evidence presentation makes them sought after in this specialized practice area.

4. Fraud Investigation and Risk/Control Reviews

Forensic accountants render such services both when called upon to investigate specific cases as well for a review of or for implementation of Internal Controls. Another area of significance is Risk Assessment and Risk Mitigation.

5. Settlement of insurance claims:

Insurance companies engage forensic accountants to have an accurate assessment of claims to be settled.

Similarly, policyholders seek the help of a forensic accountant when they need to challenge the claim settlement as worked out by the insurance companies. A forensic accountant handles the claims relating to consequential loss policy, property loss due to various risks, fidelity insurance and other types of insurance claims.

6. Dispute settlement:

Business firms engage forensic accountants to handle contract disputes, construction claims, product liability claims, infringement of patent and trade marks cases, liability arising from breach of contracts and so on.

What characteristics should a Forensic Auditor possess?

- Out of the Box Thinking
- Strong Visualization and Imagination
- Curiosity
- Persistence
- Detail-oriented
- Inquisitiveness
- Creativity
- Discretion
- Skepticism
- Confidence and
- Sound professional judgement.

What Skills should a Forensic Auditor possess?

1. Auditing standards, procedures and related methodologies

2. Accounting & Business reporting systems
3. Information Technology
4. Data Analytics
5. Criminology
6. Legal Framework
7. Litigation processes & procedures
8. Investigative Techniques
9. Evidence gathering
10. Network of professional contacts in related fields' viz. enforcement, regulatory bodies, law, industry, peers etc.

A forensic accountant should possess not only the broad knowledge of accounting principles, practice and standards but also the knowledge of insurance, banking civil and criminal law and human psychology.

A Forensic Auditor must be open to consider all alternatives, scrutinize the details and at the same time see the big picture. In addition, a Forensic Auditor must be able to listen effectively and communicate clearly and concisely in a timely manner.

Opportunities for Members and Those Involved in Fighting Fraud

Frauds are of such vicissitude and far reaching effects that it would be unthinkable to include every type or even all major types of frauds. However certain common situations in which members are likely to find themselves in have been envisaged and briefly described below:

1. **Conventional Investigation assignments as a continuation of audits.** These are typical SAP 4 situations where the audit findings have revealed certain anomalies and there is a suspicion of fraud or error. The management may ask the auditors to extend their audit to apply such extended or modified procedures as may be necessary to assess, evaluate and determine the nature and extent of fraud. This kind of assignment is a regular investigation and needs no elaboration. Such investigations could cover cash embezzlements, asset losses, revenue leakages through inflated or replicated invoices, suppression of income, inflation of liabilities, deflation of receivables and the list could go on and on.

2. **Investigations by Statutory authorities.** Investigations in respect of violations under any provision under the Income Tax Act, Companies Act, could be required by any of the respective authorities. Even Police, CBI, CID and the Economic Offences wing could need the services of chartered accountants. Such services could include determination of claims from investors of all kinds, assessment of funds lost or misappropriated, non-compliance of prescribed procedures, bank frauds and any other economic offence where knowledge of accounting, record-keeping and relevant applicable laws could be useful. In the recent well

published scams such as Harshad Mehta scam, C R Bhansali, Neek Leeson, and Ketan Parikh, large number of chartered accountants have been asked to provide valuable insights as to the nature and methodology of the frauds perpetrated.

3. **Bank frauds**. This area has the highest potential of fraud. The raw material is money itself. Frauds can be perpetrated within a bank itself or by outsiders. Insiders may manipulate funds, loans, and apply teeming and lading between favored accounts. Outsiders could defraud a bank by furnishing fabricated, duplicated or altered demand drafts, cheques, bills of exchange, and other negotiable instruments. Apart from these borrowers also often cheat banks in hypothecation agreements by inflating inventories or even providing substandard or spurious stocks with little or no value. Chartered Accountants may find themselves as auditors, investigators, or a part of the inspection team. These days even pre facility audits are asked to be carried out. These are audits in the garb of investigations to ensure that funds are going into safe and reliable hands

4. **Business risk evaluation**. This is another area of professional opportunity for chartered accountants. Every business venture is always fraught with risks. What varies is the degree and extent of the risk. Take for example a case where a company has to undertake a new project for which it requires a large finance say Rs 100 crores. In the current financial markets there are plenty of consultants offering a plethora of services. Very often such means of financing are obtained through consultants not very well known to the borrowers and possibly of dubious credentials. They offer new and untested financing schemes through banks or financing institutions or IDBI, or RBI, etc. In such situations sometimes upfront or advance payments are to be made which run in substantial amounts. In such circumstances either the financial officers of the company who could be chartered accountants or audit firms may be asked to inquire into the feasibility of the scheme as well as the reliability of the consultant. Since the stakes involved are generally high, such assignments offer a challenging opportunity for chartered accountants to earn the appreciation of the clients. Similar situations could arise when a new vendor, or a new client or a new venture s to be entered into and the company wants to ensure that there is no risk. In

All such situations the bottom line is to ensure that the client minimizes its chances of being duped.

5. **Insurance claim frauds**. Claims for loss of stocks and loss of profits of large values, particularly exceeding Rs 5 crores are usually surveyed in detail by most insurance companies. More often than not these claims are inflated, with or without intention. In such situations as well chartered accountants could be called upon to review, inquire and investigate into frauds.

6. **Compliance verifications**. There are so many situations where specific guidelines or directives have been laid down for use of funds. For example a large trust may be given a donation of Rs 10 crores for a project say providing for orphans and widows. The donor may want an assurance that the funds donated have been appropriately used. It is possible that

this could turn out to be a thriving ground for frauds and misappropriation of funds. Similarly a hospital may have been given funds for a specific ward with conditions. There could be misrepresentations and false reports. A business may have a remote site where certain activities may be in progress. A possibility of misuse of resources is also likely.

Chapter 5
Detecting Red Flags

The author and creator of Sherlock Holmes [Sir Arthur Conan Doyle] said that "detection is, or ought to be, an exact science, and should be treated in the same cold and unemotional way."Forensic investigation involves looking beyond the obvious. A normal accountant act like the policeman the forensic investigator role is akin to the CID/CBI and looks for signs which indicate abnormal and unusual behaviour. Such signs are referred to in forensic accounting parlance as red flags.

Buddhism refers to three kinds of poisons 'anger, greed and ignorance'. If not checked they all eventually lead to wrongdoing. A symptom or a 'red flag' will surface in some form or the other where any of these three evils are present.

Red Flags are sign or warning of any impending danger or inappropriate behaviour. Red Flags do not necessarily indicate the existence of fraud however are indicators that caution needs to be exercised while investigating the situations. Red Flags are classified in the following categories

- **Financial performance red flags:** Theyinclude aggressive goals and performance measures, both at the individual and company-wide levels. When a certain level of performance is mandated, by the boss, Investors, the bank, or otherwise, there can be a temptation to turn to fraud to meet these goals.

Companies whose financial performance suggests the possibility of fraud might include some of these signs:

- Significantly outpacing competitors in the industry
- Outstanding results when the rest of the industry has suffered a downturn
- Unusual financial ratios when compared to competitors
- Persistent cash flow problems, even when the company has regularly reported profits
- A pattern of similar audit adjustments proposed year after year

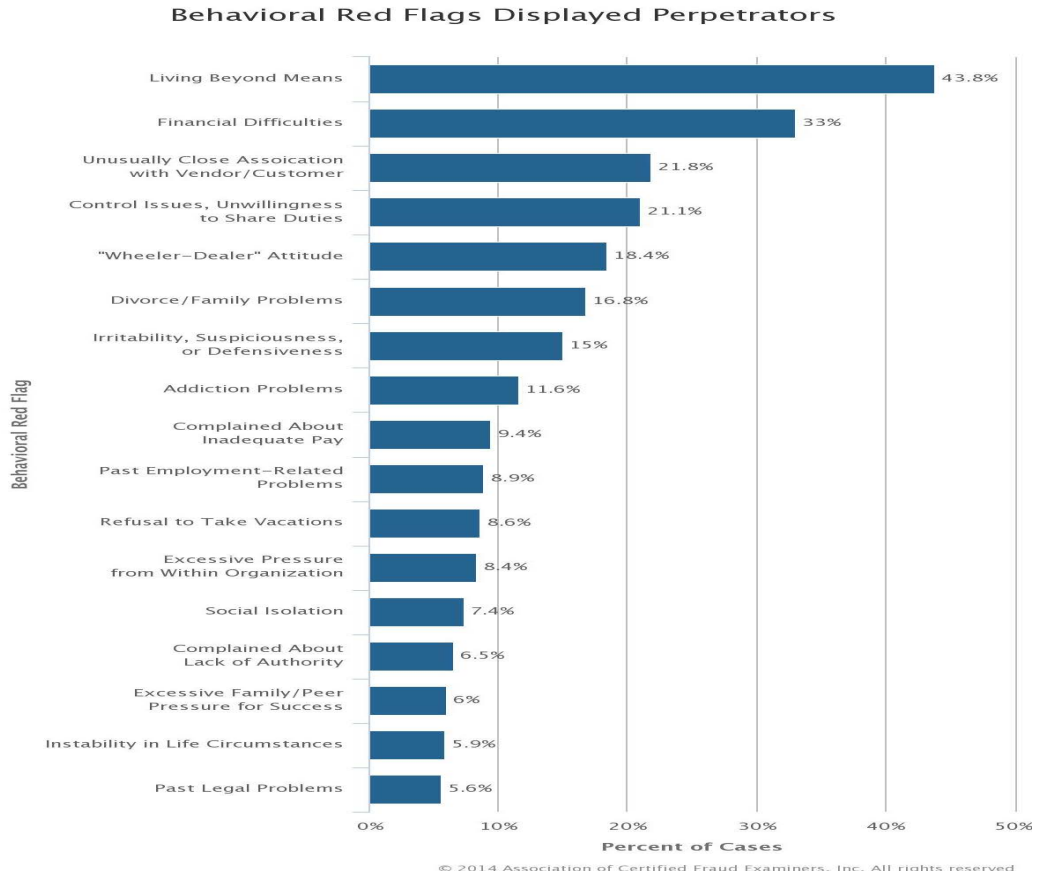
- **Accounting system red flags:** They refer to the organization of the accounting system and the level of internal controls that are in place. A good, secure accounting system cannot exist without internal controls, and the company cannot be free from error and fraud without such controls.. Some of the basic red flags that might be noted in a company's accounting records include:
    - Unusual timing of the transaction. This includes the time of day, the day of the week, or the season.

- Frequency of transactions. Transactions that are occurring too frequently or not frequently enough are suspicious. Each company has its own operating patterns, and the transactions should be booked accordingly.
- Unusual amounts recorded. Take notice of whether an account has many large, round numbers entered. Consider whether some of the transactions in the account are far too large or far too small.
- Unusual amounts recorded. Take notice of whether an account has many large, round numbers entered. Consider whether some of the transactions in the account are far too large or far too small.
- Questionable parties involved. Payment being made to a related party? Is the company paying large sums to a vendor whose name is not easily recognizable or is not a normal vendor of the company

➢ **Operational red flags:** They highlight how a company does business each day. Do things run smoothly, minimizing the chance for errors and problems? Or are things managed in such a fashion that errors go unchecked and employees do whatever they want, whenever they want?

➢ **Behavioural red flags:** They include behavioural patterns of the employees.

In "Report to the nations on occupational Fraud and Abuse' by ACFE identified the behavioural indicators displayed by Fraud Perpetrators. The below figure shows the distribution of those red flags. Approximately 44% of fraud perpetrators were living beyond their means while the fraud was ongoing, and 33% were experiencing known financial difficulties. Other common red flags were an unusually close association with a vendor or customer (22%), displaying control issues or an unwillingness to share duties (21%), a general "wheeler-dealer" attitude involving shrewd or unscrupulous behaviour (18%), and recent divorce or family problems (17%). These six red flags were also the most common behavioural indicators in each of ACFE's last three studies.



- **Structural red flags:** They relate to the way that a company is set up and the policies and procedures that are in place. Those very systems create opportunities for fraud each day. Employees become familiar with operations, and they begin to understand what accounts are unmonitored, which areas of the company are poorly supervised, and what size of transaction that creates added scrutiny.
- **Personnel red flags**: They refer to the employment policies and procedures within a company, including hiring procedures, advancement policies, employee monitoring programs, and disciplinary standards.

Appendix 3 of SA 240 'THE AUDITOR'S RESPONSIBILITIES RELATING TO FRAUD IN AN AUDIT OF FINANCIAL STATEMENTS' contains examples of certain Red Flags i.e. examples of circumstances that may indicate the possibility that the financial statements may contain a material misstatement resulting from fraud. They are as follows:

Discrepancies in the accounting records, including:

- Transactions that are not recorded in a complete or timely manner or are improperly recorded as to amount, accounting period, classification, or entity policy

- Unsupported or unauthorized balances or transactions
- Last-minute adjustments that significantly affect financial results
- Evidence of employees' access to systems and records inconsistent with that necessary to perform their authorized duties
- Tips or complaints to the auditor about alleged fraud.

Conflicting or missing evidence, including:

- Missing documents
- Documents that appear to have been altered
- Unavailability of other than photocopied or electronically transmitted documents when documents in original form are expected to exist
- Significant unexplained items on reconciliations
- Unusual balance sheet changes, or changes in trends or important financial statement ratios or relationships – for example, receivables growing faster than revenues
- Inconsistent, vague, or implausible responses from management or employees arising from inquiries or analytical procedures
- Unusual discrepancies between the entity's records and confirmation replies
- Large numbers of credit entries and other adjustments made to accounts receivable records
- Unexplained or inadequately explained differences between the accounts receivable sub-ledger and the control account, or between the customer statements and the accounts receivable sub-ledger
- Missing or non-existent cancelled checks in circumstances where cancelled checks are ordinarily returned to the entity with the bank statement Missing inventory or physical assets of significant magnitude
- Unavailable or missing electronic evidence, inconsistent with the entity's record retention practices or policies
- Fewer responses to confirmations than anticipated or a greater number of responses than anticipated
- Inability to produce evidence of key systems development and program change testing and implementation activities for current-year system changes and deployments.

Problematic or unusual relationships between the auditor and management, including:

- Denial of access to records, facilities, certain employees, customers, vendors, or others from whom audit evidence might be sought

- Undue time pressures imposed by management to resolve complex or contentious issues
- Complaints by management about the conduct of the audit or management intimidation of engagement team members, particularly in connection with the auditor's critical assessment of audit evidence or in the resolution of potential disagreements with management.
- Unusual delays by the entity in providing requested information
- Unwillingness to facilitate auditor access to key electronic files for testing through the use of computer-assisted audit techniques
- Denial of access to key IT operations staff and facilities, including security, operations, and systems development personnel
- An unwillingness to add or revise disclosures in the financial statements to make them more complete and understandable
- An unwillingness to address identified deficiencies in internal control on a timely basis.

Others:

- Unwillingness by management to permit the auditor to meet privately with those charged with governance
- Accounting policies that appear to be at variance with industry norms
- Frequent changes in accounting estimates that do not appear to result from changed circumstances
- Tolerance of violations of the entity's code of conduct.

Red flags that are "Indicia of Fraud" are nothing but symptoms or indicators of situations of frauds. They do not necessarily indicate the existence of fraud and hence the auditor should exercise caution in forming an opinion before investigating. The following are some of the red flags which examiners are likely to come across and understand.

- Lack of Corporate Governance
    - Absence of rotation of duties or prolonged exposure in the same area
    - no written policies and/or procedures
    - lack of Internal Controls or casual approach to reported internal control lapses
    - frequent or unusual Related Party transactions (not arm's length)
    - Close nexus with vendors, clients, or external parties - There would be a conflict of interests if an employee, particularly at a senior level, were to have close relations with a client.

- Questionable Accounting Activities
  - Management override of Internal Controls
  - unreconciled subsidiary & General Ledger accounts
  - continuous adjustments of book to physical inventories
  - topside Journal Entries
  - Excessive number of manual checks
    - Stale Items in Reconciliations- In bank reconciliations, deposits or checks not included in the reconciliation could be indicative of theft. Missing deposits could mean the perpetrator absconded with the funds; missing checks could indicate one made out to a bogus payee.
    - Excessive Voids - Voided sales slips could mean that the sale was rung up, the payment diverted to the use of the perpetrator, and the sales slip subsequently voided to cover the theft.
    - Excessive Credit Memos - Similar to excessive voids, this technique can be used to cover the theft of cash. A credit memo to a phony customer is written out, and the cash is taken to make total cash balance.
    - Common Names and Addresses for Refunds - Sales employees frequently make bogus refunds to customers for merchandise. The address shown for the refund is then made to the employee's address, or to the address of a friend or co-worker.
    - Increasing Reconciling Items - Stolen deposits, or bogus checks written, are frequently not removed, or covered, from the reconciliation. Hence, over a period of time, the reconciling items tend to increase.
    - General Ledger Out-of-Balance - when funds, merchandise, or assets are stolen and not covered by a fictitious entry, the general ledger will be out of balance. An inventory of the merchandise or cash is needed to confirm the existence of the missing assets.
    - Adjustments to Receivables or Payables - In cases where customer payments are misappropriated, adjustments to receivables can be made to cover the shortage. Where payables are adjusted, the perpetrator can use a phony billing scheme to convert cash to his or her own use.
    - Excess Purchases - Excess purchases can be used to cover fraud in two ways:
      - Fictitious payees are used to convert funds
      - Excessive purchases may indicate a possible payoff of purchasing agent

- Duplicate Payments - Duplicate payments are sometimes converted to the use of an employee. The employee may notice the duplicate payment, then he or she may prepare a phony endorsement of the check.
- Ghost Employees - Ghost employee schemes are frequently uncovered when an auditor, fraud examiner, or other individual distributes paychecks to employees. Missing or otherwise unaccounted for employees could indicate the existence of a ghost employee scheme.
- Employee Expense Accounts - Employees frequently conceal fraud in their individual expense account reimbursements. These reimbursements should be scrutinized for reasonableness and trends, especially in the area of cash transactions on the expense account.
- Inventory Shortages- Normal shrinkage over a period of time can be computed through historical analysis. Excessive shrinkage could explain a host of fraudulent activity, from embezzlement to theft of inventory.
- Increased Scrap - In the manufacturing process, an increased amount of scrap could indicate a scheme to steal and resell this material. Scrap is a favorite target of embezzlers because it is usually subject to less scrutiny than regular inventory.
- Large Payments to Individuals - Excessively large payments to individuals may indicate instances of fraudulent disbursements.
- Write-off of Accounts Receivable - Comparing the write-off of receivables by customers may lead to information indicating that the employee has absconded with customer payments.

- **Sudden Losses.** A company doing quite well suddenly makes huge losses. While there could be genuine reasons, mismanagement of funds and resources are more likely. These losses are likely to have been there all along simmering under window dressed accounts.
- **TGTBT syndrome.** TGTBT stands for Too Good To Be True. This indicates that lovely glossy report may be furnished whereas in real terms there are gloomy conditions.
- **Generation of 'orphan' funds.** Funds which are held in a fiduciary capacity and for which there is no accountability are thriving places for frauds. Funds collected by trusts or donations in cash collection boxes are typical examples where there is no accountability on either side. Neither does the donor concern himself about the usage of the funds nor does the beneficiary have a direct claim or even awareness in respect of such funds. However such funds can Familiarization with Red Flags in Detection of Frauds.
- **Disaster situations:** Accidents where books have been lost, or damaged, or

catastrophes such as fire, earthquake, floods etc. are other places where fraudsters can feast.

- **Missing Documentation.** This is the surest sign of fraud and practically every situation of missing records either has been created to suppress a fraud or if such a situation happens to emerge it is used to engineer a fraud.
- **Chaotic conditions.** As a corollary of disaster situations, conditions where accounts are in arrears, messy state or unreconciled, by and large are artificially created. The reason given normally is shortage of staff or resources, but this is more of an excuse.
- **Behavioral Issues**
  - failure to take vacations
  - living beyond one's means
  - Insider trading
  - early arrival – late departure
  - Irrational behavior. Behavior which is not becoming of the employees' position and which does not keep in mind the decorum of an office often stems from deep rooted insecurity which could be symptomatic of fraudulent intentions.

  The perpetrator will often display unusual behavior, that when taken as a whole is a strong indicator of fraud. The fraudster may not ever take a vacation or call in sick in fear of being caught. He or she may not assign out work even when overloaded. Other symptoms may be changes in behavior such as increased drinking, smoking, defensiveness, and unusual irritability and suspiciousness.
- **Complaints** - Frequently tips or complaints will be received which indicate that a fraudulent action is going on. Complaints have been known to be some of the best sources of fraud and should be taken seriously. Although all too often, the motives of the complainant may be suspect, the allegations usually have merit that warrant further investigation.

YELLOW FLAGS

These are indications of authorized activities which are flagged because of their unusual nature. These may be perfectly legitimate activities which are worth checking as they may also be indications of fraudulent activity. Examples of such activities are

1 Unusually high transactional amounts on a debit credit card transaction

2 Login to a system or application from an unusual IP or Location

Such transactions are used to enforce preventive measures or exception reporting e.g. Banks now call up the card holder to verify if high volume transactions or transactions from a different location or a foreign location are genuine before authorization

GREEN FLAGS

Green Flags are in many ways the converse of Red Flags. They are a part of the TGBT syndrome referred to earlier. (TOO GOOD TO BE TRUE). Examples include

- Unusually high returns provided by an investment
- High Profit Margins for a company which are way above the industry average
- Specific companies performing very well when the industry is in a slump

Like Red Flags these are only indicators and are not conclusive evidence of fraudulent activity and need to be investigated before reaching a conclusion.

Chapter 6
Process of Forensic Accounting

Each Forensic Accounting assignment is unique. Accordingly, the actual approach adopted and the procedures performed will be specific to it. However, in general, many Forensic Accounting assignments will include the steps detailed below.

A Forensic Auditor must initially consider whether his/her firm has the necessary skills and experience to accept the work. Forensic audits are highly specialized, and the work requires detailed knowledge of fraud investigation techniques and the legal framework.

Step 1. Initialization

It is vital to clarify and remove all doubts as to the real motive, purpose and utility of the assignment.

It is helpful to meet the client to obtain an understanding of the important facts, players and issues at hand. A conflict check should be carried out as soon as the relevant parties are established. It is often useful to carry out a preliminary investigation prior to the development of a detailed plan of action. This will allow subsequent planning to be based upon a more complete understanding of the issues.

Fraud audits begin with an initialization process. Internal business owners or managers, government agencies or other businesses may require a fraud audit on a company. Reasonable expectation must exist in order to conduct a fraud audit. Fraud auditors will review each request on a case-by-case basis to determine if circumstances exist whereby fraud may be going on. Incompetent accounting or handling of financial information does not necessarily indicate fraud; intent is an essential element for fraud to exist.

Step 2. Develop Plan

The forensic audit team must carefully consider what they have been asked to achieve and plan their work accordingly. This plan will take into account the knowledge gained by meeting with the client and carrying out the initial investigation and will set out the objectives to be achieved and the methodology to be utilized to accomplish them.

Planning a fraud audit will occur if auditors determine enough improprieties exist in a organization's financial or business operations. Auditors will gather information about the organization and begin a review process of the company. Each approach to fraud audits is different, primarily because fraudulent schemes come in different varieties or situations. Auditors must also try to determine who is involved in perpetrating the fraud. Gathering evidence and connecting individuals to specific events can also help auditors develop an audit plan for fully investigating a company.

The objectives of the investigation will include:

- 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 fraudster(s) involved
- quantifying the financial loss suffered by the client
- gathering evidence to be used in court proceedings
- Providing advice to prevent the reoccurrence of the fraud.

The investigators should also consider the best way to gather evidence – the use of computer assisted audit techniques, for example, is very common in fraud investigations.

Step 3. Obtain Relevant Evidence

Depending on the nature of the case, this may involve locating documents, economic information, assets, a person or company, another expert or proof of the occurrence of an event.

In order to gather detailed evidence, the investigator must understand the specific type of fraud that has been carried out, and how the fraud has been committed. The evidence should be sufficient to ultimately prove the identity of the fraudster(s), the mechanics of the fraud scheme, and the amount of financial loss suffered. It is important that the investigating team is skilled in collecting evidence that can be used in a court case, and in keeping a clear chain of custody until the evidence is presented in court. If any evidence is inconclusive or there are gaps in the chain of custody, then the evidence may be challenged in court, or even become inadmissible. Investigators must be alert to documents being falsified, damaged or destroyed by the suspect(s).

Evidence can be gathered using various techniques, such as:

- testing controls to gather evidence which identifies the weaknesses, which allowed the fraud to be perpetrated
- using analytical procedures to compare trends over time or to provide comparatives between different segments of the business
- applying computer assisted audit techniques, for example to identify the timing and location of relevant details being altered in the computer system
- discussions and interviews with employees
- Substantive techniques such as reconciliations, cash counts and reviews of documentation.

Step 4. Perform the analysis

The actual analysis performed will be dependent upon the nature of the assignment and may involve:

- calculating economic damages;
- summarizing a large number of transactions;
- performing a tracing of assets;
- performing present value calculations utilizing appropriate discount rates;
- performing a regression or sensitivity analysis;
- utilizing a computerized application such as a spread sheet, data base or computer model; and
- utilizing charts and graphics to explain the analysis.

Step 5. Reporting

Issuing an audit report is the final step of a fraud audit. Auditors will include information detailing the fraudulent activity, if any has been found. This report provides external business stakeholders with information regarding the organization's business operations. Government agencies may also wish to see the audit report. Significant fraudulent activity may result in civil or criminal charges against the individuals conducting the fraud.

The client will expect a report containing the findings of the investigation, including a summary of evidence and a conclusion as to the amount of loss suffered as a result of the fraud. The report may include sections on the nature of the assignment, scope of the investigation, approach utilized, limitations of scope and findings and/or opinions. The report will include schedules and graphics necessary to properly support and explain the findings.

The report will also discuss how the fraudster set up the fraud scheme, and which controls, if any, were circumvented. It is also likely that the investigative team will recommend improvements to controls within the organization to prevent any similar frauds occurring in the future.

The forensic auditor should have active listening skills which will enable him to summarize the facts in the report. It should be kept in mind that the report should be based on the facts assimilated during the process and not on the opinion of the person writing the report.

Step 6. Court proceedings

The investigation is likely to lead to legal proceedings against the suspect, and members of the investigative team will probably be involved in any resultant court case. The evidence gathered during the investigation will need to be presented at court, and team members may be called to court to describe the evidence they have gathered and to explain how the suspect

was identified. It is imperative that the members of the investigative team called to court can present their evidence clearly and professionally, as they may have to simplify complex accounting issues so that non-accountants involved in the court case can understand the evidence and its implications.

Chapter 7
Interviewing Skills and Techniques

7.1 Introduction

Interviewing and reporting are critical skills for anti-fraud professionals. Knowing how to conduct effective interviews and identify deception can make or break a fraud examination.

Reporting the results of an examination clearly and thoroughly supports the credibility of you and your work, and makes your findings more actionable.

Interviewing and report writing are both critical skills necessary when conducting an internal investigation.

This chapter explores the strategies necessary to conduct a successful interview, from the initial planning stages to obtaining signed statement, and handling problems which may arise during the process.

Effective interviewing is a function of both – a well-structured interview and a well prepared interviewer. Successful interviewers typically excel in interpersonal relations and can identify verbal and non-verbal clues of deception.

7.2 Overview of an Effective Interview

In any Fraud investigation, forensic accountants are asked to help management, board of directors, regulatory authorities, or law enforcement officials to determine the facts regarding complex financial matters. An effective interview is essential for gathering facts and steering the investigation in the right direction.

Knowledge of effective interviewing techniques is essential for most types of forensic investigations. The forensic accountant cannot just rely on paper trails, computer databases, and documents to provide evidence. In most cases, the accountant must acquire information from people possessing critical information.

Through interviews the forensic accountant can obtain information that identifies key issues of a case. Leads can be developed to other sources of evidence.

Interviews are used to obtain information about and to understand the allegations and to verify facts. These may take the form of formal or informal interviews.

For formal interviews, notes were taken and/or recordings were made. In some instances, the person is asked to sign the interview notes. If the interview is of importance to a particular allegation, the interviewee is informed that he or she would possibly have to confirm his or her statement at a later date.

The investigation team also conducts numerous informal interviews to collect information relating to documents and activities. Informal interviews were not recorded although hand written notes may be taken. These interviews are conducted for obtaining background information, understanding the nature of the fraud, obtaining background information on the suspected perpetrators, understanding their possible motives and even their behavior patterns.

Information about the personal backgrounds of those involved can be obtained in interviews. Interpersonal relationships can be uncovered. Possible motives can be explored. Interviews can be used to obtain the cooperation of victims and witnesses.

In forensic cases evidence is often gathered piece by piece. Interviewing is often an important step in putting the pieces together.

To be successful, an interview should be thorough. It requires strategic planning, relevant questions and an objective interviewer.

Interviewers can enhance their credibility by focusing on information that the interviewee should know, as opposed to guessing during the interview and thereby wasting the time of the participants by asking questions that the interviewee could not know. By remaining objective and fair, the interviewers can better gain the confidence of the interviewee.

An effective interviewer should be an active listener, as well as an active observer. Both are learned skills that can be studied and improved with practice. Active listening means not only listening more than talking, but really hearing what is being said and how it is being communicated. Sometimes what is not being said is equally as important as what has been said by the interviewee.

It always is recommended that only one person should be interviewed at a time. The interviews usually should begin with neutral witnesses and move to corroborating witnesses. The actual suspects of the case normally are interviewed toward the end of the interview process; however, other options may be considered depending on the nature of the case.

In some circumstances, interviews with suspects may be conducted early in the investigation if it appears that evidence may be destroyed, if the suspect is leaving the company, or if threats to other witnesses are being made.

Many other possibilities exist where a suspect (or suspects) may have to be interviewed before all pertinent documents are obtained and reviewed and before other fact witnesses are interviewed. In most every organization, there are people who are willing to share information if they can remain anonymous.

In a number of cases, confidential sources provide information through employee hotlines and anonymous letters. Additionally, former employees may provide valuable information through letters of resignation and exit interviews.

Forensic accountants also should consider that confidential sources of information may have a

hidden motive for providing information. Former spouses, business partners, employees, neighbors, and friends may know specific details. However, the reasons for providing such information may be suspect. The confidential source may be providing information that is intended to discredit or embarrass the target.

A forensic accountant should weigh the benefits of relying on the evidence against the risk of potential damage to the case if the information proves false. To the extent possible, information received from confidential sources should be corroborated through independent investigation.

An interrogation generally is viewed as a process of questioning with force, moving toward a denial of the incident or a confession. In many occasions, a simple fact-gathering interview may evolve into an interrogation with the unsuspected perpetrator of the alleged illicit activity.

The dividing line between interviews and interrogations is not always clear-cut. Interviewers should be prepared for a wide variety of circumstances in a forensic engagement and should remain objective, fair and act with integrity.

Practitioners who are not experienced in forensic investigation and who do not consult with counsel before undertaking an investigation expose themselves to potential ethical violations and/or serious legal consequences.

Forensic specialists are fact-finders who may appear to lose their objectivity if they assume the role of interrogator seeking a confession. Although a confession may be elicited based on the evidence produced by the forensic accountant, interrogation normally is reserved for experienced specialists such as law enforcement officers.

7.3 The Interview Process

7.3.1. Collection and Collating Data.

7.3.2. Purpose of the interview.

7.3.3. Time and Place for the interview.

7.3.4. Preparation for the interview

7.3.5. Recording the interview

7.3.6. Initiate the interview

7.3.7. Different types of interview questions

7.3.8. Process of taking notes during interviews

7.3.9. Concluding the interview

7.3.10. Documenting the interview

7.3.1. Collection of Data

The initial steps taken upon the initial discovery of suspected fraud are critical and should be taken with thoughtful consideration.

Forensic accountants should advise their clients to secure data, documents, and information before initiating the interview process. Once people learn that an investigation may be under way, any delay in securing electronic and documentary evidence may result in the alteration, destruction or deletion of documents or computer data.

Gathering this evidence requires that proper chain of custody procedures be followed to ensure the integrity of the evidence, especially if such evidence is to be eventually relied upon in a legal proceeding.

Collection, Organizing and Collating data is the very first step to be taken, even before making an interview plan. Data is available in various forms and can be gathered from multiple sources like phone records, CC TV footage, ERP access records, system login details, access card details and others.

Facts can be derived from business records of parties involved or external sources like government, industry and market databases. These should be coded andstored in a database for retrieval. Knowledge of information systems and database management computer programs can be a valuable aid to a forensic auditor in collecting, organizing, and summarizing the large volume of facts and related documents.

Financial modeling languages are specifically designed for this purpose andhave many built-in features to aid the user in developing pro forma financialstatements. Powerful database software is required for large cases with manydocuments. Sophisticated statistical techniques are sometimes applied to analyze the data gathered in an investigation. These methods are more advanced than the basic statistical techniques. With the help of advanced statistical software, users can employ techniques and analyze the data, financial and non financial to draw up an effective interview plan.

7.3.2. Purpose of Interviewing

An interview can best be described as a professional conversation conducted with a specific purpose or goal in mind. The thrust of an effective interview is to gain knowledge and information that is relevant to the investigation.

The primary purpose of most interviews is to gather evidence through facts and other information supplied by witnesses. Interviewing is performed throughout an investigation. With each successive interview, the interviewer should obtain background information about the witnesses, the subject matter of the investigation, and the potential suspects. Efforts should be made during the interviews to identify new records and additional witnesses.

Interviews generally should strive to answer basic questions: who, what, where, when, how and why.

An interview plan and theme should be developed before conducting the actual interviews. Presumably, an investigative plan already exists to outline the nature of the case; list of potential witnesses; a preliminary order of interviews; key issues to resolve; appropriate data, documents, and information to obtain; and investigative measures that should be conducted before interviews begin.

The interview plan should complement the investigative plan. Interviewers should therefore become familiar with the investigative work already completed, and the Interviewers also should honestly assess their own strengths and weaknesses to determine if they are properly prepared and capable of conducting the interviews.

The key elements for an investigative plan are

- The investigative team should develop and agree upon the plan before the first interview;
- The plan must be flexible enough to incorporate continual changes dictated by information unearthed at each stage of the engagement; and
- The team should meet regularly during the engagement to consider the possibility of changes in the interview program.

In terms of developing the interview strategy, an investigator should include the following:

- Whom to interview within the organization, considering both key and non-key personnel;
- Whom to interview outside the organization, considering both key and non-key third-party individuals;
- Timing of interviews, incorporating time to review documents and other information discussed and analyzed during interviews; and sequencing of interviews.

While the investigative team members may not want to reveal that they suspect fraud, they need to provide a reason for wanting to talk with potential interviewees. The reason cited should be honest but does not necessarily have to disclose concerns of fraudulent activity.

Examples of reasons to undertake these types of interviews include:

- This is part of a special-purpose audit;
- This is part of a process or accounting system improvement study;
- This is connected with an internal control study;
- We need to understand further details about a specific financial transaction; or
- Certain accounting procedures have generated some concerns.

7.3.3. Setting of Time and Place

Many interviews fail to gather enough information to address the issues raised in a forensic

matter because of inadequate preparation, or because insufficient time is allowed to complete the interview.

Normally an interview is scheduled and a fixed time is set for the initiation and completion. If possible, sufficient time should be allowed to conduct the interview with the time of completion left open. If a set time is established, the person interviewed may be overly focused on the ending time, thereby restricting a flow of information.

Ideally, the interview should be conducted as soon as the alleged impropriety has been discovered.

When arranging an interview, a location should be chosen to ensure privacy and to minimize interruptions. The use of cell phones should be discouraged.

Care should be taken to ensure that the person being interviewed has access to an exit that is not blocked by the interviewers. This is a safety consideration, but also may be a consideration to demonstrate the voluntary nature of statements.

7.3.4. Preparing for an Interview.

What to consider? Depending on the situation, there are many factors that need to be considered before undertaking an investigation.

Coordination with someone from Human Resources, Security and the Information Technology departments typically is undertaken before the interview process.

Forensic accountants should resist the temptation to initiate interviews without considering the significant legal implications that may arise. Working under the direction of counsel protects the forensic accountants from overreaching or unwittingly crossing the line. For example, interviews may be protected by legal privilege if the forensic accountant has been retained by counsel. Privileged conversations are kept confidential and may be protected from further inquiry or disclosure. Without this protection, forensic accountants may be forced to disclose inaccurate or slanderous information that may wrongly harm an individual (or individuals), thereby exposing the forensic accountant to negative legal ramifications.

Each situation presents a different set of circumstances. And each situation presents complicated legal issues that forensic accountants, by themselves, are not equipped to handle without legal guidance.

Ideally, interviews should be conducted by two people. And, the plan should outline the goals of the interview, who will be the lead interviewer, who will be taking notes, the role of the second interviewer, the subject areas and key points to cover, as well as safety considerations.

7.3.5. Recording of the Interview

If the decision is made to record interviews, proper and reliable recording equipment is required and a chain of custody for the recordings will be necessary. If recorded statements

are used in a later proceeding, the recordings will have to be authenticated and any transcriptions will have to be reviewed for accuracy.

While most recording equipment uses a digital format, the digital recordings can easily be altered. Therefore, the original recordings must be retained where a proper chain of custody and retention can provide assurances that the original recording has not been changed. Eg date and time logs.

Extreme care should be taken when making work copies of the original recording. Surreptitious recordings also are fraught with significant legal issues.

7.3.6. The Interview

The initial contact with the person to be interviewed is the first, but not last, chance to set the tone of the interview and begin the important rapport-building process.

Introductions should be polite and professional, with appropriate handshakes. Other physical contact can be easily misinterpreted and should be avoided. The identity of the interviewers should be disclosed and the identity of the person interviewed and others present should be confirmed.

During the introductory phase of the interview, interviewers should clearly state the purpose, preferably in general terms as opposed to specific terms.

The stated purpose should be logical, easy for the respondent to accept, and easy for the interviewer to explain. It should be stated that the results of the interview may also be disclosed to third parties.

Once introductions have been made, interviewers should begin with asking simple questions to put the witness at ease and help to build a rapport. Background questions should include asking their name, address, phone number, title, how long they have been in that position as well as what their duties are. During the introductory phase of the interview, sensitive questions and emotive words should be avoided. Forensic accountants may want to consider asking the person being interviewed if anyone has talked to them about the reason for the interview or if allegations have been made.

Depending on the issue being investigated, the interviewer may want to gather information regarding the target of the investigation. Such information may include work habits, personal lifestyle, usual activities, as well as any unusual behavior. It also is important for the interviewer to obtain the interviewee's basis of knowledge for his/her statements. By encouraging longer answers, interviewers can better assess the verbal, non-verbal, and physical reactions of the interviewee in order to gauge baseline reactions. Challenging information and statements at this point in the process is not recommended.

Interviewers should approach sensitive questions very carefully and should not react to statements made by the interviewee. Interviewers should not express shock, disgust or similar emotions. And, interviewers should remain nonjudgmental, fair and objective. While the

interviewers are observing the verbal and nonverbal actions of the interviewees, it should be remembered that the interviewers also can demonstrate powerful messages by their own verbal, nonverbal and physical actions.

While initial contact should be polite and professional, it is just as important to maintain firm control over the interview process. The interviewers should be viewed as in charge and with a mission to accomplish, that is, to resolve the pertinent issues. The topic of the interview should be controlled to maintain the parameters of the subject matter. Some interviewees may attempt to wrest control of the interview by omitting key information, offering evasive answers, or engaging in direct deception.

7.3.7. Types of Questions and Sequence

(a) Informational Questions

Informational type questions are designed to be non-confrontational and non-threatening. These questions are designed to gather information. Informational questions should be unbiased in nature. Such questions are used that are unlikely to cause defensiveness or hostility. These questions should be asked to develop facts in the order of their occurrence.

Only one question should be asked at a time. Interviewers should be asking straight forward and frank questions while allowing sufficient time for the interviewee to respond. It is appropriate to assist the interviewee to recall events; however, answers should not be suggested. To facilitate recall and responses, the interviewers may consider showing the person copies of data, documents, or information.

Questions can be repeated or rephrased for verification and interviewers should make certain that the answers are thoroughly understood. The interviewee should be afforded opportunities to verify and qualify answers.

Interviewers should be attempting to separate facts from inferences in their questioning by ascertaining the interviewee's basis of knowledge. In other words, the interviewers will want to determine whether a person is answering a question based on firsthand observation and knowledge, or whether the knowledge obtained from other persons (second-hand information). It also is recommended that interviewers have the interviewee summarize the facts in his or her own words in order to reduce any misunderstandings.

E.g. Where do you think there is wastage of money in the Company? Do you think there is abuse of position/authority?

(b) Open Questions

Open questions are questions where yes or no answers are not appropriate, and may need elaboration. Open questions invite wide ranging answers. Such questions encourage a monologue and narrative type response. This technique is used to get a quick summary of what is known about a matter.

When an interviewee is offering a narrative or explanation, interviewers should not interrupt the process. Important clues often are obtained by allowing the interviewee to narrate a series of events.

In addition, the interviewers can begin the "norming" process by observing how the interviewee is reacting to the statements. Open-ended questions always are encouraged to keep people talking; however, most interviews will use a combination of open and closed questions.

E.g. What do you think is the led to these losses? What is your opinion as to how they could have been avoided?

(c) Closed Questions

Closed questions are designed to require a precise answer, usually "yes" or "no." or a one word answer. As example, closed questions can be used to establish dollar amounts, dates, times and locations.

Closed questions should be avoided during the informational part in an interview where rapport building is important. However, such questions can be used extensively during the conclusion phase of the interview.

Keep in mind that a series of closed questions may tip the hand of the interviewer by revealing information about the subject matter. An overuse of closed questions also can expose the knowledge and tactics of the interviewers, which may not be desirable.

E.g. What time did you arrive at the office at the day in question? What day did the particular incidence take place?

(d) Leading Questions

In contrast, leading questions are questions that contain an answer as part of the question. Leading questions can be used to confirm facts that already are known.

By answering well-designed leading questions, the interviewee is confirming information by answering the question. An example of a leading question would be "When you made the telephone call to your boss, what did he say to you?" Leading questions often are not allowed in courtroom situations, but they can be an effective technique during the interview process.

A leading question is a question that suggests the answer it wants. Eg. What did you plan to achieve when you passed that entry? What did you do when you went into that area?

(e) Double Negative Questions

Double-negative questions should be avoided. This is because they are confusing and often suggest an answer opposite to the correct answer.

E.g. since you did not have the access nor the authority to pass that entry you shouldn't have done that should you? You are not aware of his inability to handle this matter effectively, are you?

(f) Complex Questions

Complex questions are questions that cover more than one topic. These questions can lead to confusion and require more than one answer. Therefore, they should also be avoided. It is also similar to a multi-part question i.e. a question which combines various different shorter questions into one utterance.

An example of a poorly worded question is: "You went to the data storage room and then you accessed the particular computer and after you took the data, what did you do?

(g) Attitude Questions

Attitude questions are those in which the attitude of the interviewer is conveyed by the structure of the question. An example would be: "Can you explain why we have heard contradicting answers to the same question?"

The attitude of the interviewer can be conveyed by a tone of voice or by intentionally altering body language exhibited by the interviewers. However, interviewers should not unintentionally exhibit internal emotions through their own verbal, non-verbal, or physical behavior.

(h) Admission Seeking Questions

These types of probative questions are used for getting an Admission. If decisions are made to proceed with confronting people with information detrimental to their best interest, the interview should be conducted with extreme care. In this phase of the interview, accusatory questions will be asked. The interviewers will use direct accusations in a statement that is not in the form of question. For example "We know for a fact that you have……."

(i) Question Sequence

It usually is best to seek general information before seeking details about a matter under investigation.

A variation of the concept is to reach backward with the questioning. This would mean that interviewers would begin with known information and then move into that which is unknown.

Skilled interviewers easily will move between combinations of methods. Effective interviewers will develop skills and confidence to move between open and closed questions to advance the information gathering process. At the same time, effective interviewers avoid confrontational and emotive phraseology that may lead to a termination of the interview.

To stimulate a desired answer or impression, an interviewer can direct the interview toward a specific point using a controlled answer technique. An example would be, "I understand you were present when ..." Another example would be, "Because you were not involved ..." Effective interviewers also will remain impartial and avoid polluting the interview by injecting their own opinions and emotions.

Plan your questions in advance, beginning with warm up questions i.e.

1. Establishing some kind of human connect – rapport building – introduction, reason for the meet etc.
2. Moving on to basic information including confirming known facts – role and responsibility etc.
3. Soft Questions – Questions that do not challenge or confront. E.g.what is the process generally followed?
4. Hard Questions – Questions that get to the point of the issue. E.g.why did you not follow the normal process?

Where relationships are likely to be strained even before you start, keep the initial phase of the interview short and tight. Right after introduction and common courtesy come swiftly to the point.

The interview should follow a logical structure establishing first the information you will need to build more challenging questions later on. Questions should be clear and to the point so that they are clearly understood. Use short questions instead of long winded and rambling ones and use each question to build upon for the next in sequence.

7.3.8. Note-Taking during the Interview

It is recommended that each interview is treated separately in the note-taking and report-writing process.

The lead interviewer should focus on the responses to questions and maintain eye contact to better assess the verbal and nonverbal responses from the interviewee. The interview partner should be taking extensive notes and be prepared to ask additional questions.

It is appropriate to carry a list of issues that should be asked and resolved during the interview. However, using a list of questions usually is not recommended as this would tend to interrupt the natural flow of the information exchange process. If proper listening and observation skills are deployed, interviewers will be able to ask logical follow-up questions upon hearing the responses from, and observing the behavior of the interviewee.

While taking notes, the interviewers should be writing down pertinent facts. If the statement is relevant, it is appropriate to write the statement made by using quotation marks so as to refer to it “ad verbatim”. But the note-taking process should not slow the interview process. The personal opinions of the interviewers should be omitted.

Recording the interview may be appropriate, however the interview should be recorded only after the same is informed and agreed to by the interviewee. The exact date, time, persons present and the fact that the interview/recording is not being conducted under duress should be clearly stated therein.

Digital records can be tampered easily and should be kept in safe custody.

7.3.9. How to Conclude an Interview

In closing, the interviewers should try to close an interview on a positive note and leave the door open for additional contact. Facts should be summarized and the interviewee should be encouraged to say whatever he/she desires.

Closing questions can be designed to elicit information about other witnesses or documents that may be useful in the ongoing investigation.

Interviewers should leave a business card and contact information with the witness. That way, the witness can reach out to the interviewers to mention something they may have forgotten during the interview or if at a later date they decide to provide additional information. In many situations, a thorough interview will identify other facts and circumstances requiring further investigation, which may lead to additional questions that were not covered in the first interview. Therefore, it is desirable to leave the interview on a positive note so that additional contact is encouraged.

7.3.10. Documenting an Interview

Written records of an interview should be prepared as soon as possible following the conclusion of the interview. Original notes should be retained for verification.

It is recommended that narrative reports be written in third person. A third-person account is where the interviewer is stating his or her recollection of the events of the interview.

The report should contain the date, time, location and persons present during the interview. An interview log is a good way of recording the times of significant events during the interview. As an example, the interview log may record when the interview commences, times of significant events during the interview such as breaks, telephone calls, and refreshments, and the conclusion of the interview.

Written reports should be thoroughly reviewed and compared to the original notes.

Personal opinions and comments should be avoided. Observations stated should be clear and relevant and important points highlighted. Breakthrough comments should be quoted verbatim so as to avoid misinterpretation.

Change in behavior of the interviewee, verbal and non-verbal red flags and other signs of deception should be detailed.

7.4 Common signs of deception and the techniques used to assess them

The Interviewer's role in an interview is normally like a subtle observer. He/She should not stare at the person being interviewed or call attention to a person's behavior. Interviewers should be observing the timing and consistency of behavior and should note clusters of behavior.

Caution should be exercised to avoid misinterpretations of behavior because of nervousness or stress that would be present in a normal interview type situation. Interviewers should also be aware of cultural differences that may lead to a misinterpretation of verbal and nonverbal reactions.

In looking for signs of deception, interviewers should be measuring and assessing a person against themselves. If a baseline of verbal and nonverbal behavior can be obtained, decisions can be made as to whether physical reactions are signs of deception.

Lying produces stress that is often manifested in involuntary verbal, non-verbal or physical reactions. In many instances, a person who decides to engage in deceptive answers will begin with omitting important information, known as lying by omission. Lying by omission produces less stress and is more difficult to identify though observation.

Deceptive persons may also attempt to mislead interviewers by vagueness, by insincere lack of memory, or by attempting to move the interviewers into other areas by not directly answering questions.

If lying by omission or intentional misdirection is identified, interviewers are then challenged to identify the deception and press for more information. Then, deceptive persons have to make a decision about continuing the deception, or answering questions truthfully. If a deceptive path is selected, then stress increases and the chances of identifying verbal, nonverbal, or physical reactions to stress are increased.

Interviewers should look for involuntary physical actions that may result from the body relieving itself of stress created by intentional deception. Examples include excessive motions with their hands, picking lint off their clothing or playing with objects while attempting to answer questions.

Deceptive behavior may be exhibited by a fleeing position described as the upper body facing the interviewers while the feet and lower portions point towards the door. There may be excessive crossing of arms and other physical reactions to evidence being presented by the interviewers.

Interviewers continually should assess behavior and compare the behavior toward a baseline established in the early parts of the interview. Other nonverbal clues can include closing the mouth tightly, pursing lips, covering the mouth with a hand, biting the lips, excessive blinking of the eyes, and chewing objects. Such persons may sometimes exhibit certain behaviors that may be an indication of deception. For example, interviewees may make dismissive motions with their hands in response to key questions, or place their hands over their mouths as if disguising or hiding the answers.

These concepts reinforce the need to properly prepare for interviews and underscore the importance of leaving interviews on a positive note to enhance the possibility of further interviews. On many occasions, the deceptive answers are not discovered until further along in the investigation.

Examples of the verbal clues of deception include changes in speech patterns such as speeding up or slowing down, talking louder, talking softer, coughing or clearing the throat.

People who often make internal decisions about whether to deceive the interviewers will repeat questions. In addition, and there may be comments regarding the interview such as complaints as to the location and time of the interview.

Witnesses may provide false oaths of honesty. Examples would be “I swear to God.” Or, they may offer character testimony such as “You can check with my wife or minister.” A person engaged in deception may answer a question with another question or may be overly respectful toward the interviewers.

Other verbal clues of deception may also include a reluctance to terminate the interview. This is because the interviewee may want to convince the interviewer of their innocence.

If the interviewers come to believe that the interviewee is engaged in deception, efforts should be made to discover the reason for such deception. Identifying the point in the interview where the deception started can yield valuable clues as to why a person is choosing deception over telling the truth. The interviewers should try to identify what triggered the change.

The motive for deception becomes an important issue to resolve with further questioning. It is possible that the person is being deceptive to aid himself or herself, or it may be possible that the person is protecting someone else. Other reasons may include that the witness has been threatened with retaliation, or that the person is hiding certain behavior such as an illicit affair.

More experienced criminals may not exhibit some of the deceptive verbal or nonverbal behaviors mentioned previously. This is because they may be aware that interviewers are looking for such indicators of deception.

These days, information can be found on numerous websites by searching terms relating to deception/ interviews. These websites describe and discuss these same physical, verbal and non-verbal signs of deception. With this knowledge, it is entirely possible that experienced criminals can further disguise their activity or even manipulate the interview process.

7.5 Admission Seeking Interviews

Although many white-collar criminals do not equate themselves with common criminals, it is nonetheless important to get them to admit to the behavior in question. In these instances, it may be easier to obtain a statement since many white-collar criminals may not believe that such behavior is criminal. This especially is true if they have not personally or directly benefitted from committing such acts.

However, if the target personally has benefited from committing the fraud (e.g., in cases where the target has stolen company funds), obtaining a confession may not be as easy if the target is an experienced criminal.

Many con artists are eager to talk to interviewers and consider the inevitable interviews as

additional challenges in their schemes. Their confidence comes from fooling victims and investigators. Interviewers need to discover information that offers interview leverage over the con artists. Dealing with experienced con artists presents unique challenges to interviewers.

These people tend to be charming and confident, while exploiting the trust and greed of their victims. They generally are intelligent, confident and experienced liars. Con artists will be sizing up the interviewers as well. They will tend to explain their conduct as a misunderstanding between themselves and the victims. They often use language that interviewers may not understand, and they do not fear interrogation. They often mix a degree of truth into their actions and they are familiar with questions that will be asked by the intended victim. They are able to produce impressive sounding facts and figures while concealing the fraud.

To meet the challenges of interviewing experienced criminals, forensic accountants should document and review the details of oral and written representations made to victims, any audio recordings made and previously existing interviews.

Interestingly, the skills exhibited by con artists to cover up crimes actually create vulnerabilities that can be exploited by equally skilled forensic accountants. By investigating and documenting previous crimes and efforts to conceal the crimes, forensic accountants can begin to establish a pattern of lying and cheating.

Many con artists have committed previous frauds, and they have used similar false explanations. Therefore, forensic accountants should become very familiar with the con artist before an interview.

If the suspected con artist is working for a particular organization, employment applications should be thoroughly reviewed. Employment applications often will contain misrepresentations that can be used to create interview leverage.

Other sources to be considered are public databases, social networking sites, system login records etc. If possible, financial transactions should be thoroughly reviewed and investigated before confronting an experienced con artist. Reviewing public-source information, obtaining information about previous cases and reviewing prior interviews, can all help a practitioner begin to establish a pattern of conduct.

Understanding how money was transferred from the victim to the subject and documenting the paper trail will give the interviewer an advantage. Absent this information, the advantage in the interview rests with the experienced criminal.

Again, a pattern of fraudulent conduct or a pattern of cheating creates interview leverage against the con artist. By establishing a pattern of lies, false representations and fraudulent documents, the forensic accountants can better address the criminal-intent issue.

Many self-confident con artists will want to talk in order to obtain knowledge of how much a forensic accountants knows. Experienced criminals will be confident in their abilities to

deceive and engage in their own questioning process to elicit information. In these situations, the interviewer should be very patient and allow for the subject to offer details in their explanations. Forensic accountants should not reveal their knowledge in the interview, and should be thoroughly documenting the representations in the notes.

Interviewers also may want to consider the possibility of multiple simultaneous interviews with witnesses and potential suspects, as opposed to single interviews. Regardless of well-intentioned admonishments to the contrary, many people will talk about an interview with friends and associates.

After the interviewing process begins, those persons who may be engaged in a conspiracy will want to talk to each other in order to get their stories straight. While manpower intensive, multiple simultaneous interviews may prevent this occurrence.

Interviewers will need to develop skills to keep the interview moving forward even if deception is chosen by the interviewee. The deception can effectively be used later as the investigation progresses and the interviews continue. The self-perceived advantages of the con artist can then be turned around and used against him or her. The con artist's self-assurance toward deceiving victims and investigators can lead to his or her downfall when information is properly handled by interviewers.

Decisions will have to be made in advance as to whether this interview will be arranged in advance or will be unannounced. Each procedure has its advantages and disadvantages and careful consideration should be made when making these decisions. An unannounced interview can be advantageous because persons will not have had time to prepare responses to questions. The tactic can be effective with inexperienced persons committing fraudulent acts. However, experienced criminals have been known to plant their defenses as the schemes are perpetrated. And, these people often will be well prepared for the confrontational interview.

Again, safety considerations should be considered when deciding the appropriate approach. As mentioned previously, interviewers should consult with legal counsel before the interview to discuss potential legal ramifications. This is especially important when planning to interview a potential target.

If a person clearly asks for an attorney, the questioning must stop. The exact words used by the person to ask for counsel and the time of the request should be recorded in the notes.

Desks located between interviewers and interviewees can be barriers to communication. Under ideal circumstances, the interview room can be arranged so that the entire body of the person being interviewed is observed. It is generally recommended that the person being interviewed have access to an exit, as opposed to the exit being blocked by the interviewers. Keep in mind that the nature of the interview may be reviewed by judges and juries in the future. For statements to be admitted, a judge will have to be satisfied that the statements were made on a voluntary basis without threats or coercion. The interviewers may be asked to

describe the settings of the actual interview in order for other persons to determine if the questions were obtained voluntarily.

If it appears that a confession is possible, interviewers may want to consider discussing minor issues discovered during the interview that the interviewee and interviewers can agree about. It is much easier to confess to minor issues. Afterwards, interviewers can move toward more significant issues.

In an admission-seeking interview, the interviewers will use direct accusations in a statement that is not in the form of question. For example, an interviewer may ask: “Our investigations have established that you ...” At this point, observations are made as to the reaction to the statement. The interviewers will interrupt alibis and denials offered by the interviewee.

Interviewers may want to establish a rationalization with the person being interviewed and to take this opportunity to discuss motives being offered. It may be appropriate to display physical evidence during the admissions-seeking interview and to obtain explanations from the interviewee. It may be appropriate to discuss other witness statements, to discuss the session and information uncovered during the interview, and to thereafter present an alternative for consideration by the person being interviewed.

After covering the explanations offered by the interviewee, interviewers will want to obtain information about how such acts were perpetrated. The specifics of each offense should be obtained, and consideration should be given to whether written statements will be prepared.

Interviewers will be looking for a benchmark admission, which would be the first time that a person is admitting to misconduct. If a benchmark admission is obtained, it should be recorded during the note-taking process, to be later memorialized in the written report.

At this point, leading questions may be employed to confirm known facts, to reinforce a rationalization, with the goal of obtaining a verbal confession. If a person begins to confess, interviewers want to elicit information to demonstrate that the accused person knew that conduct was wrong at the time of commission.

Sometimes, persons who have been coached will deny that they knew the conduct was wrong at the time that they were performing the act in question. This knowledge is very important when trying to establish intent, which is an element of fraud. Without intent, fraud cannot be committed. The interviewers also will want to obtain facts for independent verification that are known only to the person.

Proper questioning should establish when the offense was committed, when the offense ended, other persons involved, and other physical evidence to be obtained. Therefore, investigators will have established the initial point of fraudulent conduct as well as when the conduct ended. Interviewers should ask and carefully document the voluntariness of the confessions.

The interviewers should ask questions concerning the state of mind of the perpetrator at the

time the offense(s) occurred. Information concerning medical conditions, alcohol use and abuse, drug use and abuse, depression, and threats or coercion should be documented. Corroborating evidence and additional interviews may be required to substantiate the confession.

7.6 Barriers to an effective interview

Interviewing is a type of Communication. Effective communication is possible only if interviewer understands the psychology of interviewing. The interviewer needs to understand the elements of conversation that inhibit the interviewee and reduce such inhibitors and use the elements which facilitate effective communication and enhance the facilitators.

An interview is like a game of poker – avoid revealing one's hands and predict cards in the subject's hands based on his reactions. Each question gives information and reveals its importance or how critical it is, hence plan line of questioning based on anticipated response.

Information exchange is the central purpose of the interview. Not too much information should be given but not too little information as to be overly evasive. The tactic of only extracting information without parting with any, normally does not work.

Inhibitor to conversation is a social –psychological barrier that impedes the flow of relevant information and makes the respondent unwilling or unable to give the required information.

The respondent may be **unwilling** due to many reasons such as

Constraint of time – the respondent may not necessarily be uncooperative,he/she may just feel better use of the time.

Ego – The interviewee feels that it is below his dignity to comment on certain aspects of the incidence.

Disapproval of interviewer - The interviewee expects to be rebuffed, insulted or embarrassed by the admission, but if interviewer shows sympathy he may welcome the opportunity to divulge the information. Accepting attitude elicits candid response.

Loss of status – The fear that the information may become public is a major deterrent and by giving the required assurance that the information will only be shared on a need to know basis a lot of hurdles can be overcome.

Etiquette – The interviewee may feel that the disclosure is inappropriate or in poor taste and avoid embarrassing, threatening or shocking answers for fear of exposing themselves. This too can be forestalled by appropriate interviewer and venue.

Trauma – The interviewee associates the event, incidence or activity to an acutely unpleasant feeling or crisis experience and is not willing to divulge due to its sensitivity.

The interviewer should also remember that there is genuine possibility that the interviewer is **willing but really unable** to provide the information required by the interviewer.

Forgetting – The interviewee may be unable to recall the incident unless it is current, memory fades over time or personal defense system reconstructs or obstructs the information by addition, distortion or omission.

Confusion - The chronology of events is mixed up or inferential confusion ie based on induction/generalization or deduction specific examples

Unconscious behavior – customs or habits, settled tendency or usual pattern of behavior, circular reaction, immediate unwitting response to another person's, non-verbal clues and acute emotional crisis – reaction to others special circumstances or emotional trauma.

Repression – repression is a mental process which deals with threat and stress by blocking experiences that might evoke anxiety or guilt- they may be truthful but actually repress the memory of the act as it may be against their moral code of ethics.

7.7 Safety Considerations

Recognition and Reduction of risk is a very important aspect of an effective interview. If a forensic accountant has reason to believe that the interview may become hostile, care should be taken to ensure that the person being interviewed has access to an exit that is not blocked by the interviewers. This is a safety consideration. But, it may also be a consideration to demonstrate the voluntary nature of statements.

It is recommended that someone at the home or office know the date, time, and location of the interview, who is participating, and the expected time of return

A contact telephone number at the destination with personal cell phone numbers should be left with someone at the home office.

Avoid situations where you are asked to meet a person alone, particularly if the person is not well known to you. Having a second person as a witness during an interview is recommended for practical as well as safety reasons. A coworker as a witness may also reduce the chances of false accusations of misconduct.

The interview should ideally be conducted in business locations during normal business hours where other persons are on the premises. In some cases interviews in hotel lobbies may be appropriate, but interviews in hotel rooms are avoidable. Interviews in bars, parking lots and private vehicles are not recommended.

If you are unfamiliar with the person being interviewed, ask for a business card. View the business card carefully and retain it for your records. Always ask for full names, addresses, contact numbers and job descriptions and try to gather this information in advance when arranging a date and time for a meeting.

An interviewer and partner always should be appropriately dressed and conduct themselves in a courteous and professional manner. Avoid disclosing personal information about yourself during the interview

Trust your Instincts. While you cannot conduct a thorough background check on the person being interviewed, a date and location of an interview can be changed if your feelings lead you to believe that something is amiss. If you're uneasy, take control of the situation until a comfort level is reached. It is easy to explain changes by saying that company policy dictates the circumstances of the interview.

When first entering a room to be used for an interview, take mental notes of the layout. In the event of a problem, is there a potential escape route available? Try to avoid situations where an angry person may strike or be in reach of other physical objects that can be used to harm.

During an interview, be aware of behavioral reactions that may indicate stress, uneasiness, or even anger, these are physical red flags. Increased perspiration, dryness of the mouth, and cracking of the voice can be indications of internal turmoil as well as other potential signs of deception.

If you listen carefully, a person under stress may provide clues to potential outbursts. Your concern should intensify if the person being interviewed makes comments about violence, excessiveness, drug use, depression, abusive relationships, anger, resentment, financial problems or threats.

A person confessing to misconduct may view his or her world as falling apart and may see the persons in the room as bearing some of the blame for the situation. Depression and anger are common in these circumstances and they may influence the thinking of the person confessing to improper conduct. Many people have expressed relief while calmly confessing to serious misconduct, but do not be fooled into complacency. As an example, a person being treated for depression may have the benefit of powerful drugs to control mood swings. What if the medication was not taken that day?

Also consider that if you arranged this interview in advance, the person may believe that he or she will be confronted with incriminating information, thereby raising the interviewee's anxiety level. The forensic accountants, as the interviewer, will most likely not know this before arrival. It is important to trust your instincts. Do not put yourself in situations where you feel uncomfortable.

7.8 Cases Studies

1. Case Study -Albretch 1995

Many fraud investigation are "blown" because of interviewing mistakes

Case in point: A corporate auditor for a national chain of gas stations uncovered a $58,000 discrepancy in the cash account during the year-end audit. He then solicited explanations for the discrepancy from both the office manager and the bookkeeper--the two employees in the best position to steal the company's cash.

The explanations given for the discrepancy did not satisfy the auditor who then declared, "I'll be back first thing in the morning to figure this thing out, and if I can't find a legitimate reason for the shortage in the cash account, heads are going to roll!"

Not surprisingly, that night someone intentionally burned the gas station to the ground. Local law enforcement officials determined the fire had been intentionally started and had originated in the office--next to the filing cabinets containing all relevant documents needed to resolve the discrepancy.

As a result, the auditor was unable to develop a case against the suspected fraudster(s) using direct evidence since all relevant source documents had literally gone “up in smoke.”

The auditor “blew” this investigation by making two common interviewing mistakes: First, he attempted to conduct the interviews without adequate preparation.

The proper sequence of events in an investigation should be:

(1) Identify discrepancy or irregularity,

(2) Review source documents and other records relevant to the discrepancy,

(3) Employ other evidence-gathering procedures such as surveillance, net worth analysis of targets, and interviews of those employees not likely to be responsible for the defalcation, and

(4) Interview suspect(s).

Mistakenly, the corporate auditor went directly from step one to step four. Consequently, it was then impossible for him to complete step two.

Second, the auditor approached the targets with an insensitive, “out-to-get-someone” attitude. An effective interviewer should be sensitive, respectful, and seeking the truth--not trying to make “heads roll.”

As this example illustrates, the ability to conduct effective interviews is critical to those responsible for detecting and investigating fraudulent activity.

Case Study

The owner of a medium-sized construction company received a “tip” from a disgruntled spouse that “Raj”--a highly-trusted, senior project manager--had an ownership interest in two vendors with which the construction company did business.

Consequently, the owner engaged a forensic auditor to conduct a review of the two vendors in question. The review revealed that the vendors had only post office box addresses, no phone numbers listed on the invoices, and did not have taxpayer identification numbers on file. The payments made to the two vendors totaled Rs. 7,50,000. Neither of the vendors was listed in the phone book.

Raj, who was also a close personal friend of the owner, had approved the payments. A search of the local business registrations revealed that both vendors in question had indeed been created by Raj. After a substantial amount of preliminary investigative work, the auditor decided to confront Raj with this information and solicit explanations.

Interview:

Auditor: "Hi, my name is Dilip. (Both shake hands and sit down.) The owner has asked me to review some of our business practices looking for ways to improve the profitability of the company. Do you have a few minutes to answer some questions?"

Raj: "Yes."

Dilip: "I appreciate your willingness to take time to speak with me. Tell me about your duties and responsibilities with the company."

Raj: "I'm a project manager. I oversee construction projects, estimate construction costs and scrutinize tenders, allot job work and approve payments."

Dilip: "How long have you been with the company?"

Raj: "About 8 years."

Dilip: "Are you satisfied with the work environment and the compensation you receive?"

Raj: "Yeah, I like working here, it feels like home."

Analysis: Raj has agreed to answer some questions relevant to improving the profitability of the company. Dilip does not immediately confront Raj with the incriminating information but instead tries to put him at ease by asking a series of non-sensitive questions. The purpose of these non-sensitive questions is to "calibrate" the subject; that is, to establish a baseline for the subject's verbal and nonverbal cues when we know he is responding truthfully to non-sensitive questions. Later in the interview--when the questions move toward more sensitive, possibly incriminating issues--we will compare the subject's verbal and nonverbal cues to those observed during the early part of the interview. This process, called calibration, can be very effective in determining whether subjects are being truthful or not.

Dilip: "The owner has asked me to look into the possibility of fraudulent activity by management and employees. Do you think fraud is a problem for business in general?"

Raj: "I have no idea."

Verbal cues: The interview is now moving toward more sensitive, possibly incriminating issues. Most informed people would acknowledge that fraud is a problem for business in general. However, since Raj is actually guilty of fraudulent activity, he is not inclined to acknowledge that fraud is a problem for business in general and would like to end the interview as soon as possible.

Dilip: "Do you think that this company has a problem with fraud?"

Raj: "No, not at all." (Leans back in his chair and looks down at the floor)

Verbal cues: Once again, Raj fails to acknowledge fraud as being a problem. He is now wondering if Dilip will eventually accuse him of fraudulent activity.

Nonverbal cues: Raj shifts his body position away from the interviewer and breaks eye contact, he does not want Dilip to see his discomfiture.

Dilip: "If employees or managers are stealing from this company, why do you think they would do it?"

Raj: "How should I know? I don't steal."

Verbal cues: Even though the question is non-accusatory, Raj feels directly attacked by the question and responds accordingly. Such "denials" to non-accusatory questions can be good indicators that the subject has "something to hide."

Dilip: "I didn't say you did. If you knew another employee was stealing from the business, what would you do?"

Raj: "I don't know, I've never really thought about it."

Dilip: "Do you know of anyone who might be stealing or taking unfair advantage of the business?"

Raj: "No, sir."

Dilip: "Suppose someone who worked here decided to steal or commit fraud. How could they do it and get away with it?

Raj: "They couldn't get away with it. They'd be caught if they stole." (Crosses legs, folds arms and stays locked in this position for some time)

Verbal cues: Raj continues to respond negatively in an effort to end the interview. Also, he answers too surely concerning whether someone could steal and get away with it. Raj does not even want to consider the possibility of fraudulent schemes as it is too close to home. Someone not involved in fraudulent activity generally has no problem verbalizing ways employees could steal from the company and not be detected.

Nonverbal cues: Raj is feeling personally attacked by this line of questioning and is dealing with the mounting anxiety by adopting a defensive, rigid and immobile position. It is very difficult to solicit a confession from a subject while "locked" in this position.

Dilip: "In your opinion, who is beyond suspicion when it comes to committing fraud at this company?"

Raj: "There is no fraud going on but if there was it could be anybody." (Looks at floor)

Dilip: "Did you ever think about stealing from the business, even though you didn't go through with it?"

Raj: "In all honesty, no."

Verbal cues: Raj is unwilling to narrow the list of prospective fraudsters; he wants the circle of suspicion to be as wide as possible. He issued an indirect denial ("There is no fraud going

on")--another indicator that he has something to hide. Someone being untruthful tends to use phrases like "in all honesty," "to tell you the truth," or "I swear to God" in an effort to increase the credibility of their responses. A truthful person tends not to use such phrases.

Nonverbal cues: Raj again breaks eye contact; it is very difficult for most people to lie while maintaining eye contact.

Dilip: "The owner has asked me to review some vendors which have been used on projects you supervise. Are you familiar with Shefali Constructron Pvt. Ltd., Chennai?"

Raj: "Vaguely, we did business with them for about three years. We don't do business with them anymore." (Takes off glasses, rubs eyes, lays glasses on the table, recrosses arms and legs)

Verbal cues: Dilip spends10 -12 minutes asking Raj about vendors known to be legitimate before asking about the first fictitious vendor. When questioned about legitimate vendors, Raj was able to recall all pertinent information. However, when questioned about the fictitious vendors, Raj suddenly had problems remembering anything about them.

Nonverbal cues: In an effort to relieve the stress created by this question, he has shifted his body position and taken off his glasses. Taking off the glasses is a form of breaking eye contact.

Dilip: "Which projects did they supply?"

Raj: "I don't recall."

Dilip: "What kinds of supplies were typically purchased from them?"

Raj: "I'm not sure. They weren't a major supplier."

Dilip: "Who is the sales rep for the company?"

Raj: "I don't remember."

Dilip: "Are you familiar with Padman Contracting?"

Raj: "Yes, we do business with them on occasion."

Dilip: "Where are they located?"

Raj: "I don't remember." (Dilip stands up and stretches.)

Dilip: "Why don't we take a break and stretch for a minute. I'm going to get myself a Coffee, would you like one?"

Raj: "No thanks, I'm fine." (Raj stands up to stretch while Dilip exits. Two minutes later Dilip reenters with Coffee in hand. Before Raj has a chance to get seated, Dilip begins questioning again.)

Verbal cues: The twofold purpose of this break in the interview is: (1) to get Raj out of the

"rigid and immobile" position, and (2) to leave Raj in the room alone and allow his anxiety level to continue to mount. Upon reentering the room, Dilip will issue a direct accusation before Raj has a chance to rebuild his defenses.

Dilip: "I have reliable information that you are the sole owner of both ShefaliConstructron and Padman Contracting, both of which are vendors you have approved payments to in the past. Is this true?"

Raj: (Silence for one long minute.)... "That's correct."

Dilip: "What are your reasons for creating and operating these two businesses?"

Raj: "My brother and I started the companies to earn some extra money to pay off some debts. I knew it was a conflict of interest to authorize purchase orders and approve payments, but there was nothing fraudulent going on."

Analysis: Catching Raj "off-guard" Dilip issues a direct accusation which Raj ponders momentarily before answering.

Dilip: "I didn't say there was. Did you approve payment of Rs. 140,000/- to Shefali Constructron Company for this invoice." (Hands Raj an invoice but Raj puts it on the table, face down)

Raj: "Yes, but that's the only one. I closed that company down two years ago."

Analysis: Raj is more likely to admit to the fraudulent invoices one at a time rather than being confronted with them all at once. Also, when admitting to fraudulent activity, it is very common for perpetrators to minimize--and lie about--the magnitude of what they have done.

Nonverbal cues: Raj does not want to look at the incriminating invoice so he puts it face down on the table. An honest person would want to look at the invoice in question for pertinent information which might exonerate him.

Dilip: "What service or product did you provide for the rs. 140,000/- you received?"

Raj: (Looks down at the floor.) "Nothing."

Analysis: Raj just admitted to the fictitious vendor scheme.

Dilip: "How many invoices did you submit from Padman Contracting?"

Raj: "Three or four."

Dilip: "Tell me about this invoice to XYX Co for 6.10 lacs." (Hands Raj an invoice but Raj puts it on the table, face down)

Raj: "Padman Contracting provided materials and labor for a project involving XYZ Co."

Dilip: "How much was the actual cost of materials and labor?" Raj: "About 1.6 lacs for materials and 2 lacs for labor."

Analysis: Raj is slowly breaking down and admitting to more and more. Raj actually feels some relief from the intense anxiety by "getting this off his chest." He likes this feeling and can extend it by continuing to admit to things. Accordingly, it is imperative that the interview not be interrupted at this point in the interview.

Dilip: "What happened to the rest of the money?"

Raj: "It went into the checking account I had opened for Padman Contracting."

Dilip: "What did you do with the 'profit'?"

Raj: "Paid off credit cards, paid medical bills."

Analysis: Dilip needs to know what Raj did with the money for two reasons. First, Raj will be more likely to sign a "statement of admission" if the statement contains his motivations for "taking" money from his employer. The fact that he had substantial financial pressures on him that caused him to do something "out of character" for him allows Raj to "save face" and facilitates his cooperation during the remainder of the investigation. Second, the employee dishonesty insurance provider will want to know what the target did with the money for purposes of estimating the probability of recovery.

Dilip: "Were you involved in any other types of unauthorized activities? Kickbacks from vendors? Selling company materials or scrap?"

Raj: "No, and after the XYZ Co. invoice I was going to quit and never do it again."

Dilip: "Are you aware of other situations where employees of this company are engaged in unauthorized or fraudulent activities?"

Raj: "No."

Analysis: Typically, if one employee is defrauding the company, others within the company are also engaged in fraudulent activity. Simply inquiring of an employee who has just admitted to fraud can be very effective in uncovering other fraudulent activity.

Dilip: "Let me summarize what you've told me. Due to financial pressures weighing on you such as credit card debt and medical bills, you set up two companies—Shefali Constructron and Padman Contracting --to generate some extra money. When you initially set up the companies, you intended to actually provide some labor and materials for the payments received, but for one reason or another, you ended up providing little or no materials and labor. The amount you took in this manner totaled about 7.50 lacs. You knew what you were doing was wrong but didn't consider it to be that big a deal. Is my summary of the situation accurate?"

Raj: "....Yes."

Analysis: Since Dilip will be converting the content of the "admission-seeking" interview into a written statement to be signed by Raj, it is important to get all the facts straight. Raj must be

willing to acknowledge that he knew that what he did was wrong and the written statement must unambiguously communicate this. Notice the absence of the words “steal” or “fraud” in Dilip’s summary. The use of such inflammatory terms makes the subject less likely to sign the written “statement of admission.” Instead of condemning the subject for his/her behavior, allow the subject to “save face” by focusing on the fraudulent act rather than the person.

Verbally acknowledge to the subject that you understand s/he was under heavy financial pressure which motivated him or her to do something “out of character.” Such an attitude will greatly increase the chances of obtaining a signed “statement of admission” from the subject. The signed statement will greatly facilitate the employee dishonesty insurance claim and any criminal or civil action resulting from the case.

Dilip: “Here’s my card, let me know if you think of anything else which might be relevant to this situation. Is there anything else you’d like to say?”

Raj: “Yeah,...What’s going to happen now?”

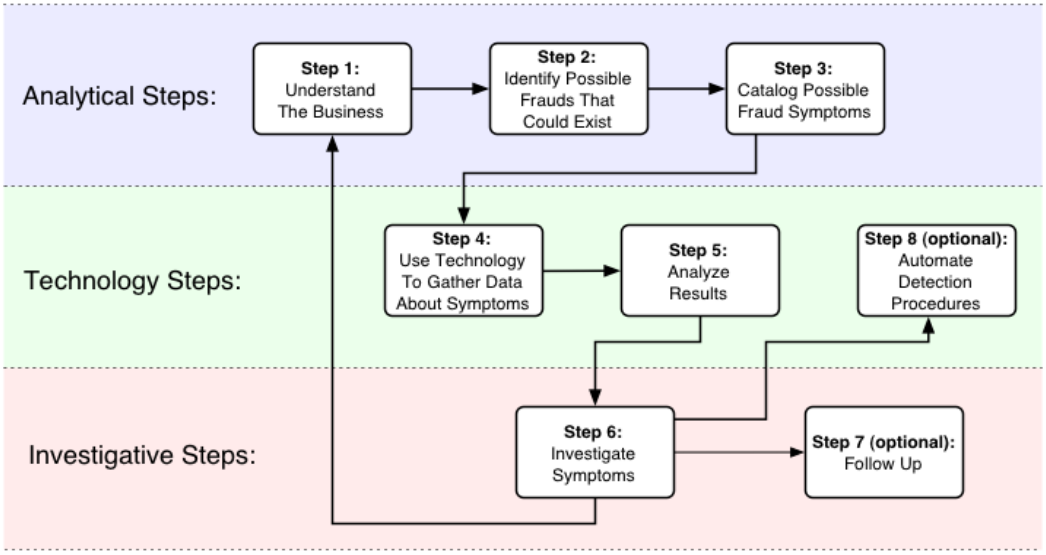
Dilip: “I’m going to put together a written statement for you to sign. Then I will report my findings to the owner of the company, and it will be his decision what happens next. (Stands up, extends hand to Raj). Thanks for taking time with me to resolve this situation. It’s good to get this all behind us so we can move on. “

7.9 Summary

1. Interview preparation is key. Devote as much time to research, collecting primary documents, question planning and rehearsal as you can.
2. Set up the interview in a way that suits the story and circumstances.
3. Lose the attitude. Even in interviews that may become adversarial, a calm, neutral demeanour and questioning style will produce better results.
4. Have a strategy for the whole interview. Always move from warm-up and broad, less threatening questions towards more precise, focused questions that will allow you to pin the interviewee down on key aspects.
5. Use data-mapping techniques to pinpoint the areas of short information and contradiction your interview needs to deal with.
6. Keep questions clear, simple and direct.
7. Establish ground rules and confirm basic information at the start of an interview.
8. Follow-up, re-phrase or reflect back to get answers that are equally clear and direct.
9. Take your time and don’t be scared of silences.
10. Handle reluctant or fearful interviewees kindly and carefully – but don’t let them off the hook.

11. Establish support structures and strategies to help you deal with threats and intimidation.
12. Use covert interviewing techniques only after careful, ethical decision-making – and be sure you have the technical skills to carry them off.
13. Never take interview answers out of context.
14. Keep in mind safety considerations.
15. Watch, Listen and Observe!

Chapter 8
Forensic Audit Techniques



Detecting fraud is difficult, especially frauds involving material financial statement misstatements, which occur only in about 2 percent of all financial statements. Fraud is generally concealed and often occurs through collusion. Normally, the documents supporting omitted transactions are not kept in company files. False documentation is often created or legitimate documents are altered to support fictitious transactions. While fraud detection techniques will not identify all fraud, the use of sound techniques can increase the likelihood that misstatements or defalcations will be discovered on a timely basis.

The Seven Recognized Investigative Tools and Techniques Used by Forensic Specialists/ Fraud Examiners

- Public Document Reviews and Background Investigations
  - Public Databases
  - MCA Website
  - Corporate Records
  - Internet
- Interviews of Knowledgeable Persons
  - Interview /Interrogation

  - Continuous process throughout an investigation
  - Gain additional information with each interview
  - Evidence from witnesses provides additional leads
  - May identify additional witnesses
  - Interview the target only after completing the interviews of the peripheral witnesses
- Confidential Sources
  - Hotlines
  - E-mail
  - Letters
  - Current Employees
  - Former Employees
  - Vendors & former vendors
  - Customers & former customers
- Laboratory Analysis of Physical and Electronic Evidence
  - physical examination
  - fingerprint analysis
  - forgeries
  - ink sampling
  - document dating
  - Computer Forensics
    - hard disk imaging
    - E-mail analysis
    - search for erased files
    - analyze use & possible misuse
    - computer software to analyze data
- Physical and Electronic Surveillance
- Undercover Operations
- Analysis of Financial Transactions

Some of the Techniques that a Forensic Auditor may use are listed below:

- General Audit Techniques
- Statistical & Mathematical Techniques
- Digital/ Electronic Techniques
- CAATT
- Data Mining

8.1 General Audit Techniques

1. Testing Defenses

Most businesses and other organizations have procedures and defenses set up to prevent the occurrence of fraud. A good initial forensic audit technique is to attempt to circumvent these defenses yourself. The weaknesses you find within the organization's controls will most probably guide you down the same path taken by suspected perpetrators. This technique requires you to attempt to put yourself in the shoes and think like your suspect.

8.2 Statistical & Mathematical Techniques

1. Trend Analysis

Businesses have cycles and seasons much akin to nature itself. An expense or event within a business that would be analogous to a snowy day in the middle of summer is worth investigating. Careful review of your subject organization's historical norms is necessary in order for you to be able to discern the outlier event should it arise within your investigation.

2. Ratio Analysis

Another useful fraud detection technique is the calculation of data analysis ratios for key numeric fields. Like financial ratios that give indications of the financial health of a company, data analysis ratios report on the fraud health by identifying possible symptoms of fraud.

Three commonly employed ratios are: -

(a) The ratio of the highest value to the lowest value (max/min);

(b) The ratio of the highest value to the second highest value (max/max2); and

The ratio of the current year to the previous year Using ratio analysis, a financial expert studies relationships between specified costs and some measure of production, such as units sold, dollars of sales or direct labor hours. For example, to arrive at overhead costs per direct labor hour – Total overhead costs might be divided by total direct labor hours. Ratio analysis may help a Forensic Auditor to estimate expenses.

8.3 Technology Based/ Digital Forensics Techniques

Every transaction leaves a digital footprint in today's computer-driven society. Close scrutiny of relevant emails, accounting records, phone logs and target hard drives is a requisite facet of any modern forensic audit. Before taking steps such as obtaining data from email etc. the forensic auditor should take appropriate legal advice so that it doesn't amount to invasion of privacy. Digital investigations can become quite complex and require support from trained digital investigators. However, many open-source digital forensics tools are now available to assist you in this phase of the investigation.

Forensic Computing is the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable in a court of law.

Digital Crime Scene Investigation involves determining what fraud events occurred by using digital evidence and has broad stages:

- Preserve & Document Scene
- Analyze/Search & Document Data
- Reconstruct & Document Fraud Event

1. Cross-drive analysis

A forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection.

2. Live analysis

The examination of computers from within the operating system using custom forensics or existing sysadmin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down. (Sysadmin - A system administrator, or sysadmin, is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers. The system administrator seeks to ensure that the uptime, performance, resources, and security of the computers he or she manages meet the needs of the users, without exceeding the budget.)

3. Deleted files

A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

4. Stochastic forensics

A method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.

Physical systems in which we are uncertain about the values of parameters, measurements, expected input and disturbances are termed Stochastic Systems.

5. Steganography

One of the techniques used to hide data is via steganography, the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the image appears exactly the same, the hash changes as the data changes.

6. EnCase

EnCase from Guidance Software is a Windows-based comprehensive and complete forensic application. EnCase is recognized as a court-validated standard in computer forensics software. Encase can have the following functionalities.

1. File signature analysis
2. Filter conditions and queries
3. View deleted files and file fragments in unallocated or slack space
4. Folder recovery
5. Log file and event log analysis
6. File type search
7. Registry viewer, external file viewer WinHex Tool: WinHex is a universal hex editor, particularly helpful in computer forensics, data recovery, low-level data editing.
    - Reduces internal investigation costs
    - Platform independent
    - Automated analysis saves time
    - Supports electronic records audit
    - Creates logical evidence files — eliminating need to capture entire hard drives
    - Previews computers over the network to determine whether relevant evidence exists:
        - Unallocated/allocated space

- Deleted files
- File slack
- Volume slack
- File system attributes
- CD ROMs/DVDs
- Mounted FireWire and USB devices
- Mounted encrypted volumes
- Mounted thumb drives

7. MD5

- Message Digest – a hashing algorithm used to generate a checksum
- Available online as freeware
- Any changes to file will change the checksum
- Generate MD5 of system or critical files regularly
- Keep checksums in a secure place to compare against later if integrity is questioned

8. Tracking Log Files

9. PC System Log

10. Free Log Tools

Name	Type	URL
fwlogwatch	Log analyzer	http://fwlogwatch.inside-security.de/
Log Parser	Log parser	http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en
Log Tool	Log parser	http://xjack.org/logtool/
LogSentry (formerly known as Logcheck)	Log analyzer	http://logcheck.org/, http://sourceforge.net/projects/logcheck/
Logsurfer	Log analyzer	http://www.cert.dfn.de/eng/logsurf/
Logwatch	Log analyzer	http://www.logwatch.org/
Project Lasso	Windows event log management	http://sourceforge.net/projects/lassolog
Swatch	Log analyzer	http://swatch.sourceforge.net/

A. Hidden data analysis: In storage media Suspects can hide their sensitive data in various areas of the file system such as Volume slack; file slack, bad clusters, deleted file spaces.

Hard Disks: The maintenance track / Protected Area on ATA (Advanced Technology Attachment) disks are used to hide information. The evidence collection tools can copy the above contents.

File System Tables: A file allocation table in FAT and Master File Table in NTFS are used to keep track of files. These entries are manipulated to hide vital and sensitive information.

B. File Deletion: When a file is deleted, the record of the file is removed from the table, thereby making it appear that it does not exist anymore. The clusters used by the deleted file are marked as being free and can now be used to store other data. However, although the record is gone, the data may still reside in the clusters of the hard disk. That data we can recover by calculating starting and end of the file in Hex format and copy it into a text file and save with corresponding extension.

Recover a JPEG file

- Open file in the hex format
- Check the file signature
- Copy From starting signature upto ending signature.

For example (JPEG/JPG/JPE/JFIF file starting signature is FF D8 FF E1 XX XX 45 78 69 66 00 (EXIF in asci Exchangeable image file format trailer is FF D9). Open the file with corresponding application.

C. Partition Tables: Information about how partitions are set up on a machine is stored in a partition table, which is a part of the Master Boot Record (MBR). When the computer is booted, the partition table allows the computer to understand how the hard disk is organized and then passes this information to the operating system. When a partition is deleted, the entry in the partition table is removed, making the data inaccessible. However, even though the partition entry has been removed, the data still resides on the hard disk.

D. Slack space: A file system may not use an entire partition. The space after the end of the volume called volume slack that can be used to hide data. The space between Partitions is also vulnerable for hiding data. File slack space is another hidden storage. When a file does not end on a sector boundary, operating systems fill the rest of the sector with data from RAM, giving it the name RAM slack. When a file is deleted, its entry in the file system is updated to indicate its deleted status and the clusters that were previously allocated to storing are unallocated and can be reused to store a new file. However, the data are left on the disk and it is often possible to retrieve a file immediately after it has been deleted. The data will remain on the disk until a new file overwrites them however, if the new file does not take up the entire cluster, a portion of the old file might remain in the slack space. In this case, a portion of a file can be retrieved long after it has been deleted and partially overwritten.

E. Free space: When a file is moved from one hard disk or partition to another, it is actually a multistep process of copying and deleting the file. First, a new copy of the file is created on the target partition. After the file has been copied, the original file is then deleted. This process also requires some housekeeping in the FAT or MFT tables. A new entry is created in the table on the partition where it has been copied, whereas the record for the deleted file is removed from the table on its partition. When a file get deleted, that space considered as free space, there also criminal can hide sensitive information.

F. Faked Bad Clusters: Clusters marked as bad may be used to hide data. In NFTS, bad clusters are marked in metadata file called $BadClus, which is in MFT entry 8. Originally, $BadClus is a sparse file which file size is set to the size of entire file system. When bad clusters are detected, they will be allocated to this file. The size of data that can be hidden with this technique is unlimited. Suspects can simply allocate more clusters.

8.4 Computer Assisted Auditing Techniques (CAATs)/ Computer Assisted Audit Techniques and Tools (CAATT)

Audit in general and fraud investigation in particular is getting complex day by day primarily due to migration to non-paper based systems. Processes and workflows are system driven and generally the entire control revolves around the computerized environment. Therefore, there is a clear trend that auditors would have to churn voluminous digitalized data as auditable records. Needless to say, auditors would therefore have to devise ways and means of verification that is commensurate with the changing times. The challenges are to examine various databases generated from different systems which may or may not be integrated.

Changing patterns of businesses, regulatory framework, scarcity of resources at auditors' disposal on one side and the ever increasing mountainous data on other hand is making audit a complex process. Use of CAATTs is, thus, indispensable to the Auditors and forensic auditors.

Computer-assisted audit techniques (CAATs) or computer-assisted audit tools and techniques (CAATTs) are computer programs that the auditors use as part of the audit procedures to process data of audit significance contained in a client's information systems, without depending on him. CAAT helps auditors to perform various auditing procedures such as:

(a) Testing details of transactions and balances

(b) identifying inconsistencies or significant fluctuations

(c) Testing general as well as application control of computer systems

(d) Sampling programs to extract data for audit testing, and

(e) Redoing calculations performed by accounting systems.

CAATTs, as the name suggests, deals with two aspects -- the CAT-Tool and CAT-Technique. While the CAT-Tool refers to use of software tool, the CAT technique insinuates enhancing the effectiveness and efficiency of audit to work with the CAT-Tool on the auditable database. Thus both are integrated part of each other like a sides of scissors and one will not be able to work without the other. Needless to say both sides have to work in tandem to be able to cut through the complex data. CAT-Tool is all about learning the syntax of a software application and will also entail a need to know about the database architecture. It deals with 'How-to' work on the database. Whereas the CAT-technique is all about the auditor's judgment to apply procedures on the database knowing auditee's environment vis-a-vis the underlying audit objective. This part deals with What-to-do with the database.

Computer Aided Audit Tools or CAATs can be broadly divided into

- Generalized Audit Software's (GAS) or
- Common Software Tools (CST)

CAATs include tools that range from basic word processing to expert systems. Computerized audit techniques range from procedures as simple as listing the data in a given file to the use of Artificial Intelligence tools to predict financial failure or financial statement structures. For instance, general productivity software such as Microsoft Word, MS Excel and MS Access can be used to support audit work including text processing, spreadsheet analysis and graphics. MS Access and other general purpose databases and data analysis tools including Oracle, Statistical Analysis Software (SAS), Structured Query Language (SQL), Crystal Report and PowerBuilder can be used as forms of generalized retrieval software (GRS) or for more sophisticated data analysis tools. Embedded Audit Modules (EAMs) are a class of CAATs that are integrated within the entity's application systems and which support real time or quasi-real time monitoring of transactions within the accounting information system.

8.5 Generalized Audit Software (GAS)

Generalized Audit Software (GAS) is a class of CAATs that allows auditors to undertake data extraction, querying, manipulation, summarization and analytical tasks. Arguably the most widely deployed class of CAATs is Generalized Audit Software (GAS). These packages are computer programs that contain general modules to read existing computer files and perform sophisticated manipulations of data contained in the files to accomplish audit tasks. They have a user-friendly interface that captures users' audit requirements and translates those user instructions or queries into program code. This is undertaken by interrogating the client's file systems or database and performing the necessary program steps. As compared to embedded audit modules, they do not require a certain level of programming expertise to design and implement the audit queries.

These are specialized software's designed for accountants fostered with audit architecture in mind. The user interface is very simple for users to follow and with that objective, GASs very often have out-of-box-integration with leading accounting / other systems. However simple it

may sound, it needs some training and experience to use them and some people do find it complex to operate.

GAS focuses on the fully exploiting the data available in the entity's application systems in the pursuit of audit objectives. GAS support auditors by allowing them to examine the entity's data easily, flexibly, independently and interactively in data based auditing. Using GAS, an auditor can formulate a range of alternative hypotheses for a particular potential misstatement in the subject matter and then test those hypotheses immediately. "What if" scenarios can be developed with the results and the auditors can examine the generated report rapidly.

Currently, the latest versions of GAS include the Audit Command Language (ACL), Interactive Data Extraction and Analysis (IDEA) and Pan audit.

Audit Command Language -ACL

ACL is the market leader in computer-assisted audit technology and is an established forensics tool. It is a computer data extraction and analytical audit tool with audit capabilities like Statistics, Duplicates and Gaps, Stratify and Classify, Sampling, Benford Analysis, using a GAS such as ACL means the auditor does not review a sample of the data, but rather reviews or examines 100 percent of the data and transactions.

8.6 Common Software Tools (CST)

Due to shortcomings of GASs, CSTs have become popular over a period. Spreadsheets (like MS Excel, Lotus, etc.), RDBMS (like MS Access, etc.) and Report writers (like Crystal reports, etc.) are few examples of CSTs. Their widespread acceptability is due to its instant availability and lower costs. While spreadsheets may be extremely easy to use due to its simplicity and versatility, other CSTs may need some practice.

Whether one uses GAS or CST, it is imperative that the auditor is aware about the manner and processes that have led to the data generation, the control environment revolving around the data and the source from where the data samples are imported into the GAS/CST.

As a part of computer-aided audit, an auditor needs to do one or more of the following.

1. Check Missing
2. Check Duplicates
3. Round Numbers
4. Repetitive Odd-Numbers
5. Classification
6. Stratification
7. Single Transactions
8. Isolated Outliers

(i) Check Missing: Here we basically try to identify the gaps in any workflow that has serial control mechanism. For example, missing cheques numbers, insurance policies numbers, and bank fixed deposit receipts, good received notes, cash receipt numbers, etc. Depending upon the availability of data vis-a-vis audit objectives, an appropriate data attribute (data field) may be selected to run this check. Missing gaps can be filtered for auditee's explanations.

(ii) Check Duplicates: the serial control numbers which ought not to be repeated are checked for duplicates. Thus all the documents (that have serial control), mentioned in the above paragraph can be checked for replication. Duplicated numbers could throw up serious gaps in the sourcing of these documents or in case they have been generated using some computerized system could mean a software bug. All such duplicated numbers need thorough detailed review to dispel any wrong doing

(iii) Round Numbers: Basically there is nothing wrong with Round numbers and it is not unusual to see many round number transactions in any commercial deals. However, sometimes round numbers are symptomatic of mysterious deals. Therefore the auditor should use some judgement to eliminate possible round number cases. For example, it is quite natural to generally spot round number transactions in monthly rentals, professional fees, audit remuneration, etc. - these transactions could be filtered out from the list of transactions with round numbers.

(iv) Repetitive Odd-Numbers: This is converse of Round-numbers. Unlike the round numbers, repetition of odd numbers (particularly repetitions at decimals levels) are very rare coincident. Unless of course there is apparent reasons say, like for Telco having promotional offer of Rs 199/- prepaid packs - but in that case, the repetitions will be by volumes and not a few stray incidences here and there. Repeated oddnumber transactions can be filtered for detailed verification and most often these will throw up some irregularities.

(v) Classification: Classification is a process of arranging data into homogenous group or classes according to some common characteristics present in the data. This analysis aid the Auditor in getting a bird's eye view to see a panoramic whole of how the data is dispersed or where the concentration lies. Classification can be combined with other appropriate CAATT checks to enable more penetrative tests.

(vi) Stratification: Stratification is a derivative of classification which involves grouping of large data into 'strata'. Strata means levels, bands or groups. Thus it involves dividing or rearranging the data within the Strata and then overviewing it to decipher the latent configuration of the database.

(vii) Single Transaction: This is self-explanatory and may need little explanation. As the name suggests, this check basically filters all the single transactions in a database. These single records could be bonafide cases or just a stray transaction inserted by opportunist beneficiary. Generally vendor account, employee account, customer

account, etc. should have multiple transactions since everyone wants regular business. Solitary transaction could be vouchsafe to exonerate sketchiness if any.

(viii) Isolated Outliers: An Isolated outlier is an observation in a data set which is far extreme in value from the others in the data set. It is an unusually large or an unusually small value compared to the others. Any database will be vitiated by incongruent records or contaminated transactions which will stick out as outliers. That happens because of its inherent nature that impedes its blending with the others in the group and will be clearly isolated with the remainders.

(a) A word of caution -- there could outliers that would creep in any database as deviations which happens in normal course and may not always mean a fraud or an error. However, as an auditor s/he will be concerned about these outliers and should review these transactions as part of audit plan.

(b) There are various ways to spot the Isolated Outliers as discussed below.

(c) Simple Charting Options

(d) Relative Size Factor

(e) RSF is the ratio of Largest Number to the Second Largest Number of a relevant set.

i. RSF = Largest Number

1. Second Largest Number

(f) For example, if we have following bank payment vouchers of Vendor XYZ

(ix) Voucher No.	(x) Rs.
(xi) SB-211	(xii) 50,000
(xiii) SB-642	(xiv) 5,00,000
(xv) SB-547	(xvi) 5,00,000
(xvii) SB-1864	(xviii) 20,000
(xix) SB-4755	(xx) 23,000
(xxi) SB-8347	(xxii) 8,500

(a) The Largest value in above table = Rs 5,00,000/- and the second largest value = Rs 50,000/-. Therefore the RSF in this case = 10 that is Rs 5,00,000 Lacs divided by Rs. 50,000/-. Per RSF theory generally any transactions where RSF > 10 are the cases of isolated outliers.

(b) Relevance of RSF:

(c) Scrutiny of individual parties account is humanly ineffective and now with most of the data available digitally how does one scrutinize the ledgers? RSF theory comes in very handy here, instantly one can calculate RSF and take sample for verification. This tool finds focus and meaning to the scrutiny. It highlights all unusual fluctuations which may be stemming from frauds or errors.

Application of RSF theory in audit

- Any set of transactions generally take place in certain range or limits. Thus there is a certain pattern of financial limits peculiar to each vendor, customer, employee, etc. These limits may not be defined, but the data can be analyzed to view a pattern. RSF captures this pattern as ratio.
- For example in case of vendor X the normal invoicing range, say is Rs. 20k to 50k per bill. If there is any stray instance of single transaction which is way beyond the normal range than that ought to be looked into. That is, in the instant case, if there is bill of Rs. 5 lacs than it naturally concerns the auditor to have a look at.
- RSF is above case will give a ratio of 10. That is. ratio of
- Rs. 5lacs (largest value) to Rs. 0.50 lacs (second largest value)
- This single instance could be case where there is some foul play or error in punching of the data (due to additional zero at the end).

Case study on use of RSF

ICE, a large multinational white goods company had set up operations in India in the year 2000 by acquiring a small local manufacturing company and expanded its operations countrywide. The investigators were called in the year 2003 / 2004 pursuant to allegations contained in an anonymous letter against the Plant Manager. Initial engagement discussion revealed that the ICE's outflows mainly comprised of labor payments, power, Capex, raw materials, job-works, R&M, etc.

The investigator first ran a check of RSF on the vendor data and got the following parties where the RSF exceeded 10.

Vendor	Max_Val	2nd Max_ Val	RSF > 10
WAP Systems LLC	25,748,906	2,059,912	12.50
Indergoll Rand Ltd	206,788,550	13,586,007	15.22
Difel Inc.	96,574,432	3,094,148	31.21
Ajmera Constructions	45,659,440	1,551,753	29.42
A-Technologies Ltd	13,478,523	705,870	19.09

A drill-down on the voucher level details of the above vendors revealed following information

Name	Doc Ref	Date	Rs.	Particulars No. Of Cases	
WAP Sys	17089343	31-Mar-01	25,748,906	WAP -ERP System	14 Capitalised
WAP Sys	18088874	06-May-02 2,059,912	WAP-system-AMC	14 for 2 years	
Indergoll	17089352	31-Mar-01 206,788,550	SW, PS, Asly-line	22 Capitalised	
Indergoll	17089353	31-Mar-01 13,586,007	P&M Erection and	22 Comm.Chgs	
Difel	17089355	31-Mar-01 96,574,432	Foaming System	16 Capitalised	
Difel	18089983	05-Jun-01	3,094,148	Foaming cryst s/w	16 Capitalised
Ajmera	17069323	15-Jan-01	45,659,440	FacBldg.,	Admn
Ajmera	17070222	02-Feb-01	1,551,753	Wing,	Stores, FGStore Interiors-Office, 18 Mng.,Conf.,Canteen
A-Techn	37852344	25-Mar-03	13,478,523	Mould qty1 - SKE	4,586 4011 Stellar
A-Techn	18088874	21-Jan-03	705,870	Mould Job wrk	4,586 HDL-5004 - 15000 nos.

Considering the information obtained, the RSF of M/s. WAP, Indergoll, Difel, Ajmera were explainable since they had basically supplied capital items which was one time large cost and subsequent bills would be for supply of services/ spares etc. and hence the cost would be much lower. However, A-Tech was a job worker and had issued over 4,500 bills. So the pattern of his general transactions were in range of 50,000 to 7,00,000/-, thus the off-beat transaction of Rs 1.34 Crores needed a review.

The investigator made inquiries of the transaction for Rs. 1.34 Cr and learnt that it was towards the cost of mould purchased from A-Tech. General review of accounting documents and supporting showed everything to be in order. He was explained that generally moulds are procured from another vendor but this one was purchased since ATech was L1. The investigator reviewed the quotes received, bid comparison, etc. and noted that indeed A-tech

was lowest. He also noted that the next bid value was about Rs 3 Crores that is more than double then the quote of A-Tech. This raised a red-flag that how was A-Tech able to supply the same mould in less than half of its competitor. He decided to inspect the asset. To cut the long story short, when he investigated into the procurement, it was found that the mould actually belonged to the ICE only which was not in use and had been discarded by the previous management of ICE and later sold as scrap to A-tech. The plant manager in connivance with the A-tech created the need for a mould which was little bit modified and put to use. The mould was however sold back to the company at much higher profit.

How to calculate RSF in MS Excel

Given data of about 1000 records extracted from Account payable system. The data consists of following relevant fields.

- Voucher No.
- Voucher Date
- Vendor Name
- Bill Amount
- Bill Number

The objective is to find out the RSF for each vendor in following format

Vendor	Max_Val	2nd Max_Val	RSF
Col _A	Col_B	Col_C	Col_D

Summarized Steps

Step 1 : Extract the maximum value for each vendor and store in a column of the work sheet - say col. B

Step 2 : Extract the second maximum value for each vendor and store in another column say col. C

Step 3 : Divide Col. 'B' by 'C' to get RSF Ratio and store result in Col. 'D'

Step 4 :Filter Col. 'D' for results where RSF is more than say 10.

Step 5 : Filter records from Database for the above results as audit sample.

Detailed Steps

Step 1 : To obtain the largest or maximum value from the data

- *Use Pivot Table Function to classify the bill-amount field of data.*
- *The classification criteria will be vendor name*

- *Classification of Bill amount field will be for "Max. Value"*

Step 2 : To obtain the 2nd maximum value from the data

- *To obtain the 2nd max value, it will be necessary to nullify the max. values obtained in Step 1 above. This can be done as follows.*
- Extract results obtain from the first step to append to the data with the maximum value for the each respective vendor. This can be done by using 'Vlookup' Function.

  Formula = Vlookup (Criteria Cell Ref, Data Source, Offset)
- Nullify the effect of the bill amount if the respective bill value is equal to the Max. value. Using the 'If' function.

  Formula = If (BillValueCellRef = MaxValueCellRef, 0, BillValueCellRef.)

  [The above formula will add to the existing database, a field with bill amount which is not a MAX.Value.]
- Repeat The First Step again to obtain the max value from the field created above. The max value now will be actually the 2nd Max. value.

Step 3 : Divide the Max Value with 2nd max Value

- This is a simple divide function **Formula = MaxValueCellRef**

2nd MaxValueCellRef

- The result obtained is RSF

Step 4 : Filter the RSF col. to extract where RSF is more than say 10

- This can be done using the Auto Filter Command of excel sheet by customizing the limits.
- The result obtained are data where RSF is more than 10.

Step 5 : Filter records from Database for the above results.

- This is same as filter command used in Step 4, except that now the filter is set on the main database.
- This data is records where the max value of bills exceeded the 2nd max value over five times.

Benford's Law

This is revolutionary theorem pro-founded by Dr. Frank Benford, an American Electrical Engineer and Physicists. Benford's Law is also popularly known as the first digit law. The law is about statistical statement regarding occurrence of numerical digits. Dr. Benford observed that in any large database generated through a ordinary process, the natural numbers

(numbers which are not limited by boundaries or non-serial nos.) follow a count of its first-left-most digit which is not in consonance with the law of probability. He asserted that the first-leftmost-digit (e.g. it is "1" in a number 1,2,3,4,5,6,7,8") follows a pattern of appearance where the lower numbers have more chance of appearing as compared to the higher numbers. According to him the appearance of first left most digit has the following frequency.

Digit	1	2	3	4	5	6	7	8	9
Frequency (%)	30.1	17.6	12.5	9.7	7.9	6.7	5.8	5.1	4.6

Thus numbers deviating from the above principle would be transactions that could are isolated outliers.

This table was compiled after sheer hard work on widely disparate populations such as a day's stock quotations, a tournament's tennis scores, the numbers on the front page of The New York Times, the populations of towns, electricity bills in the Solomon Islands, the molecular weights of compounds, the half-lives of radioactive atoms and much more.

How does this help auditors? The one word answer for this is 'phenomenally'. The application of this law in auditing can lead to amazing discoveries in terms of errors or frauds. Data validation and analysis of a new dimension is now possible. Most accountants or embezzlers would not know that any error or fraud is very likely to be caught or trapped by digital analysis using this amazing theorem. This is because a material error or a fraud, influences a natural number population and consequently the data set loses its digital properties as predicted by Benford and a digital analysis would easily throw up the anomalies for an auditor to concentrate upon. Thus this law facilitates an auditor to virtually focus his attention directly on fraud or error prone areas. Research studies have shown that a digital analyses are successful about 68 % of the time with the limited knowledge that humans possess as of date, as regards this law and its potential.

8.7 Data mining techniques

It is a set of assisted techniques designed to automatically mine large volumes of data for new, hidden or unexpected information or patterns.

- If You Know Exactly What You Are Looking for, Use Structured Query Language (SQL).
- If You Know Only Vaguely What You Are Looking for, Turn to Data Mining.

Data mining techniques are categorized in three ways: Discovery, Predictive modeling and Deviation and Link analysis. It discovers the usual knowledge or patterns in data, without a predefined idea or hypothesis about what the pattern may be, i.e. without any prior knowledge of fraud. It explains various affinities, association, trends and variations in the form of conditional logic. In predictive modeling, patterns discovered from the database are used to predict the outcome and to guess data for new value items. In Deviation analysis the norm is found first, and then those items are detected that deviate from the usual within a given

threshold (to find anomalies by extracted patterns). Link discovery has emerged recently for detecting a suspicious pattern. It mostly uses deterministic graphical techniques, Bayesian probabilistic casual networks. This method involves "pattern matching" algorithm to 'extract' any rare or suspicious cases.

Data mining commonly involves four classes of task:

- Classification - Arranges the data into predefined groups with the help of algorithms
- Clustering - Is like classification but the groups are not predefined, so the algorithm will try to group similar items together
- Regression - Attempts to find a function which models the data with the least error. A common method is to use Genetic Programming.
- Association rule learning - Searches for relationships between variables.

8.8 Laboratory Analysis of Physical and Electronic Evidence

- **Computer Forensics**
  - hard disk imaging
  - E-mail analysis
  - search for erased files
  - analyze use & possible misuse
  - computer software to analyze data
- **Protection/Validation of Evidence**
  - Federal Rules of Evidence
  - Chain of Custody
  - Altered & Fictitious Documents
  - physical examination
  - fingerprint analysis
  - forgeries
  - ink sampling
  - document dating

Chapter 9
Using Excel for Forensic Audit

MS Excel software needs no introduction; it's a simple application which most of us use every day -time-in and out. The versatile spreadsheet is available almost on all machines and seldom one will find an accountant / auditor not using it. While mostly it is popular for making statements, charts, etc., it can conveniently be also used as CAAT. This article is to facilitate to make best use of whatever little is known by user about MSExcel.

Some of the important MSExcel-functions that are useful as CAAT for audit / investigation are described below.

- 'IF'
- 'IF' in combination with 'AND'
- 'IF' in Combination with 'AND' & 'OR'
- 'CountIF' and 'SUMIF'
- 'SUMIFS'
- 'VLOOKUP'
- Pivot Table Function
- Formula Auditing

Note: The above list is not exhaustive but is only an illustrative one. There are many other useful functions and the users may develop skills once he/she starts practicing them. Also it needs to be noted that there are several ways in MS Excel to achieve the same results; therefore this article attempts to only explain a few of them.

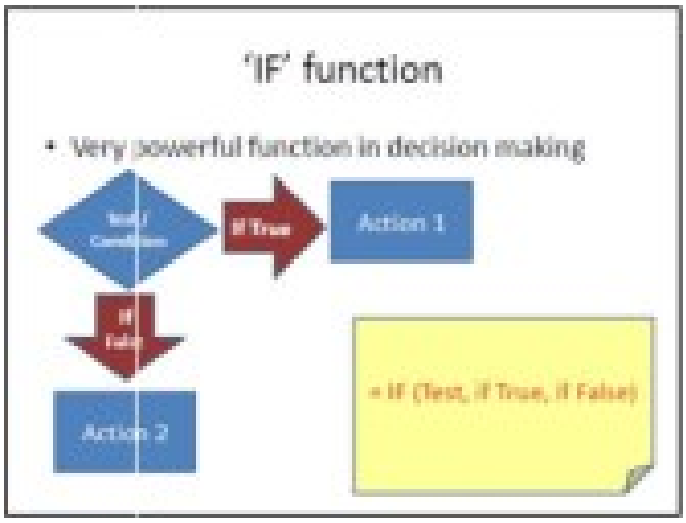
The above functions are explained in detail with its corresponding application in audit / fraud investigations.

The 'IF' Function

The IF Function along with its derivative usage with 'AND' / 'OR' can be useful for:

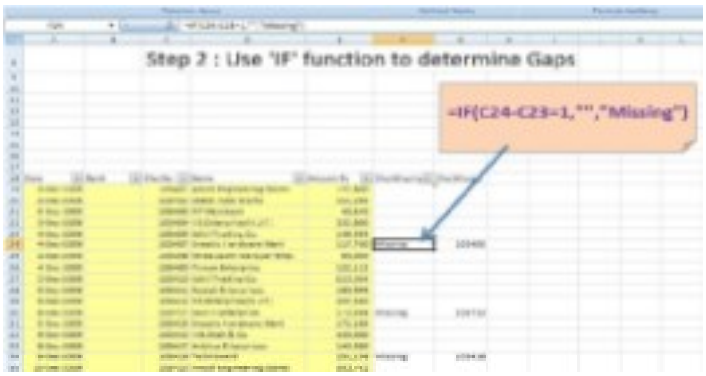
- Detecting Gaps
- Finding Duplicates
- Locating Multiple Records
- Flagging Records

- Ageing Analysis or Advance Analysis
- Extracting Records meeting certain criteria (Combination with filter commands or with Pivot Table commands)



Example of 'IF' Function:

The given data is list of cheques issued and the objective is to determine gaps of missing cheque numbers.

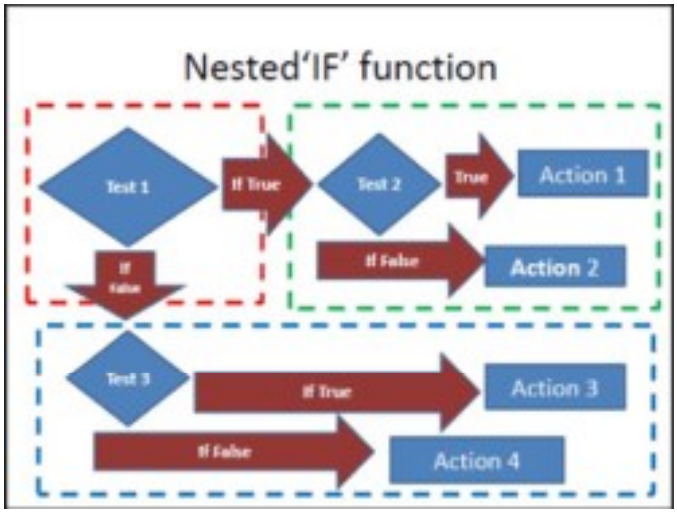


For complex operations, another 'IF' function can be used within an 'IF' function. This is known as Nested-IF function which is explained as follows :

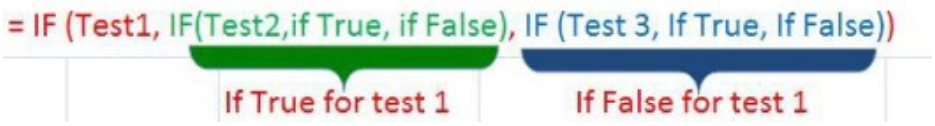
The Nested 'IF' functions

That is using IF within IF Function.

Here we use multiple tests (queries/ questions) in serial order and depending upon the response of preceding test another logical test follows. The nested-IF function can be explained as follows:



Syntax of Nested IF



= IF (Test1,

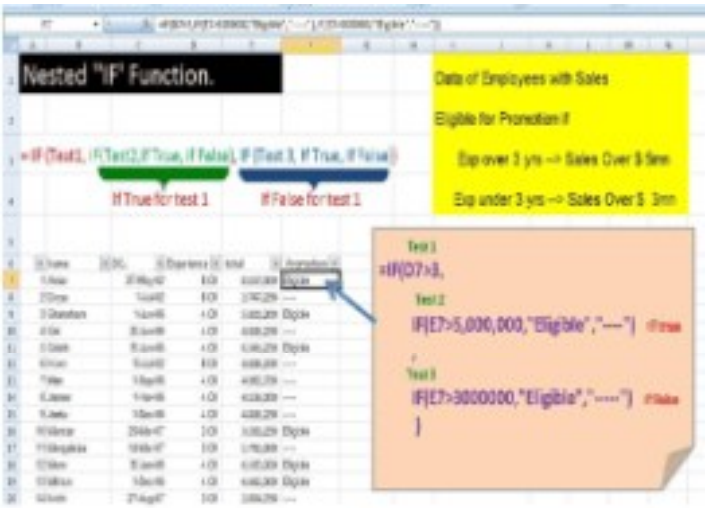
if true IF [Test2, if true,if false], if false IF [Test 3, if true, if false])

There can be maximum of 64 nested 'IF's

Example of Nested-IF function

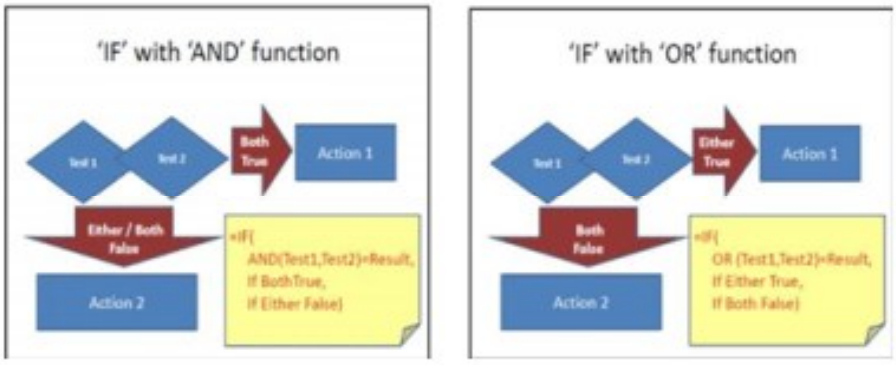
The given data is list of sales team with their date of joining, years of experience and sales achieved during a period. A salesman is entitled to promotion depending upon his/her experience and sales achieved. If his experience in under 3 years, he/she is eligible if the sales are over $ 3mn and for others the eligibility sales criteria is $ 5mn. The objective is to flag 'Eligible' status in Col-F

The Eligible and Not-Eligible employees can be filtered separately to check with the promotions given.



Using 'IF' function in combination with 'AND'/ 'OR'

Sometimes we need to have two or more tests that needs simultaneous confirmation for logical actions, this can be done by using the 'AND' or 'OR' with the 'IF' function. These results can also be achieved using the Nested-IF functions, however sometimes it may be easier to use 'AND'/'OR' functions. The 'IF' in combination with 'AND'/'OR' are explained below:

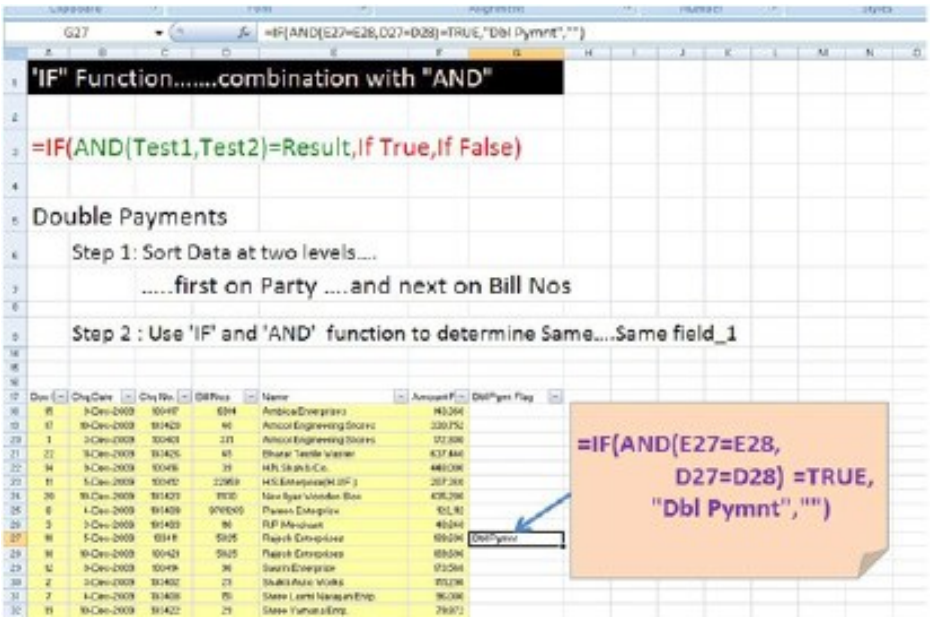


Syntax of 'IF' function used in combination with 'AND'

=IF(AND(Test1,Test2)=Result,IfTrue,If False)

Example of 'IF' function used in combination with 'AND' :

The given data is a list of payments stating details of cheque nos., bills reference (against which the payments are made) and the name of vendor with the amounts. Here is order to establish multipayments, one need to compare the vendor names and the bills numbers. When there is match for both criteria (Name and Bill No.) then double payment flag is set.



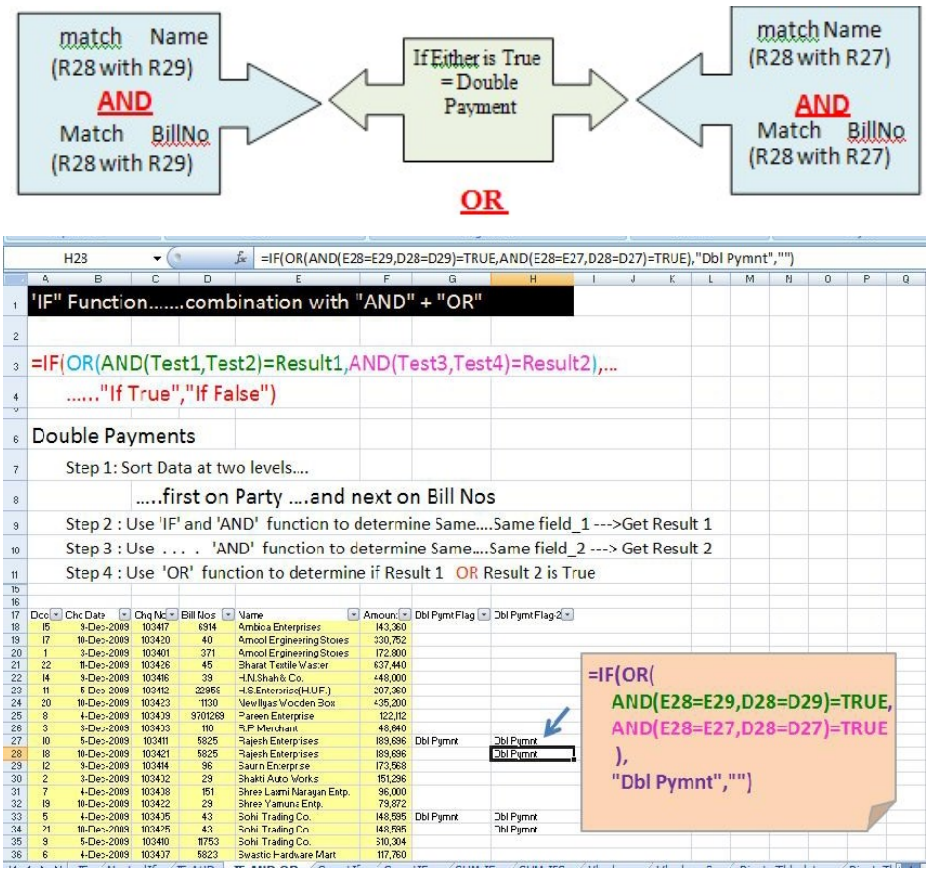
Syntax of 'IF' function used in combination with 'OR'

=IF(OR (Test1,Test2) = Result, If Either True, If Both False)

Example of 'IF' function used in combination with 'AND' + 'OR'

Continuing with the same example as above, it can be seen that we are able to flag only one of the two records of double payments. On applying filters, though we have details of the double payments, we cannot show both the records. It happens because we are comparing the record on current line with a below-line item (in above example Row27 is compared with Row28).Therefore to flag both the records (or if there more than 2 than all the records), we need to compare the current line item with line-item above and line-item below. That is, say for record at Row28, we need to check Row28-with-Row29 AND Row28-with-Row27. If either combination matches then that record needs to be flagged for "DblPymnt".

To simplify (at Record at Row28) we need to :



On filtering the "DblPymnt" records, we are able to get all the bills that are paid more than once.

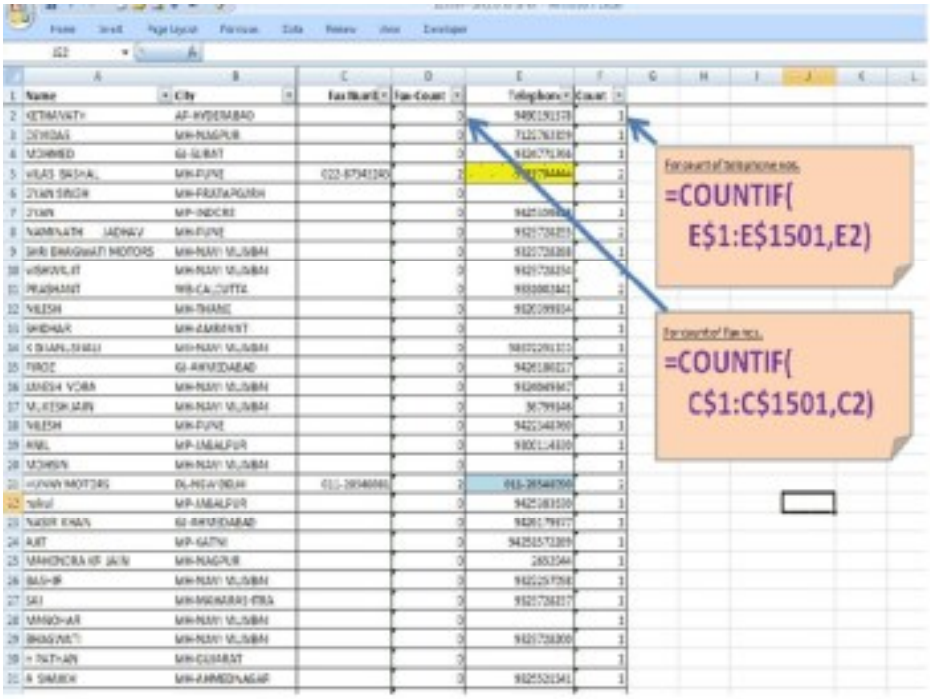
The 'COUNTIF' Function

This function counts the Tnumber of records satisfying user criteria.

This function is extremely useful in analysis of master databases (vendors, customers, employees, etc.) to determine whether there is nexus between them. For example common telephone numbers, fax nos., contact person references, email_ids., etc. can give a clue of linkages. This function can be coupled with 'filter' command to give instant results.

cSyntax Of 'COUNTIF' Function:

= COUNTIF (criteria_range, criteria,) Example Of 'COUNTIF' Function:



The given data is of vendors details -Vendor_name, city, fax-nos. and telephone nos.

By using the 'Countif' function we can count (say for Row2) how many times the fax number (in cell C2) is repeated in the entire Col-C (the count is stored in Col-D).

Similarly we can also count how many times the tel_no. (in cell E2) is repeated in the sentire Col-E (the count is stored in Col-F).

Thereafter set filters for:

- fax-counts more than 2 and
- tel-counts more than 2 following result is obtained…….the linakages bet' the parts are highlighted.

H1504

	A	B	C	D	E	F
1	Name	City	Fax Numb	Fax-Count	Telephone	Count
5	VILAS BASHAL	MH-PUNE	022-87543245	2	9819794444	2
21	HUNNY MOTORS	DL-NEW DELHI	011-28548081	2	011-28548090	2
164	VIBA MOTORS	MH-PUNE	022-87543245	2	9819794444	2
167	SHAILESH	GJ-AHMEDABAD	0271-44558677	2	9327484160	2
172	JAYDEEP ENTERPRISES	GJ-AHMEDABAD	0271-44558677	2	9327484160	2
212	PAWANJEET SINGH	DL-NEW DELHI	011-32648611	3	9212230990	3
274	GURUNANAK MOTORS	DL-NEW DELHI	011-32648611	3	9212230990	3
730	PERU MOTORS WORKS	TN-TIRUVARUR	04366-251696	2	9443383686	2
731	SWARANJIT SINGH CHHATWA	DL-NEW DELHI	011-28548081	2	011-28548090	2
740	JASBIR SINGH	DL-NEW DELHI	011-32648611	3	9212230990	3
880	G NAGESHWAR	KA-BANGALORE - 3 (East	040-6654 6700	2	9886673199	2
942	MANJUNATH	KA-BANGALORE - 2 (Wes	040-6654 6700	2	9886673199	2
992	KALIAPERUMAL	TN-TIRUVARUR	04366-251696	2	9443383686	2
1502						

The filtered records can be copied on another sheet and sorted on fax_no. / tel_no to get the proper result :

Home Insert Page Layout Formulas Data Review View Developer

C19

	A	B	C	D	E	F	G
1	Name	City	Fax Number	Fax-Count	Telephone 2	Count	
2	HUNNY MOTORS	DL-NEW DELHI	011-28548081	2	011-28548090	2	
3	SWARANJIT SINGH CHHATWAL	DL-NEW DELHI	011-28548081	2	011-28548090	2	
4	PAWANJEET SINGH	DL-NEW DELHI	011-32648611	3	9212230990	3	
5	GURUNANAK MOTORS	DL-NEW DELHI	011-32648611	3	9212230990	3	
6	JASBIR SINGH	DL-NEW DELHI	011-32648611	3	9212230990	3	
7	VILAS BASHAL	MH-PUNE	022-87543245	2	9819794444	2	
8	VIBA MOTORS	MH-PUNE	022-87543245	2	9819794444	2	
9	SHAILESH	GJ-AHMEDABAD	0271-44558677	2	9327484160	2	
10	JAYDEEP ENTERPRISES	GJ-AHMEDABAD	0271-44558677	2	9327484160	2	
11	G NAGESHWAR	KA-BANGALORE - 3 (East)	040-6654 6700	2	9886673199	2	
12	MANJUNATH	KA-BANGALORE - 2 (West)	040-6654 6700	2	9886673199	2	
13	PERU MOTORS WORKS	TN-TIRUVARUR	04366-251696	2	9443383686	2	
14	KALIAPERUMAL	TN-TIRUVARUR	04366-251696	2	9443383686	2	
15							

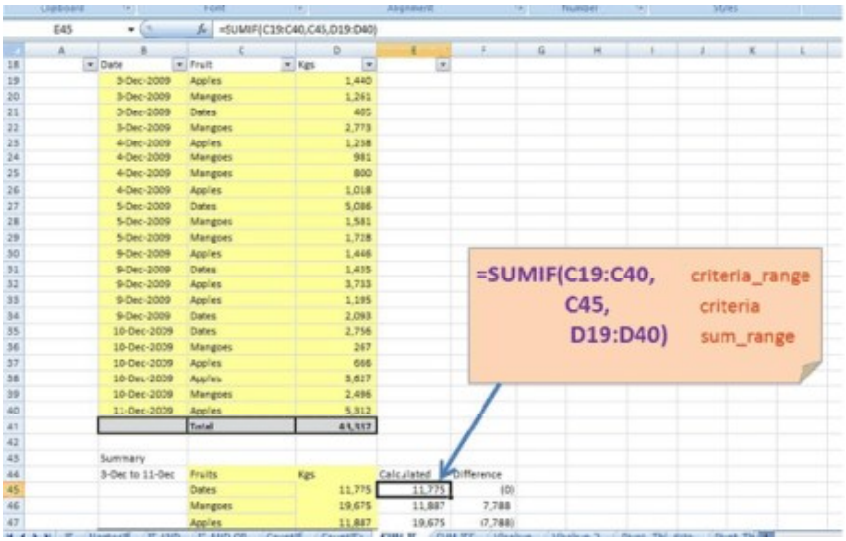
The 'SUMIF' Function this is an extension of widely used 'Sum' function but here the 'SUM' is combined with 'IF'. Thus summation can be obtained of selected records satisfying user defined criteria. This function operates the same way as Pivot Table Command. However,

Pivot Table function is not on real-time basis (one need to refresh to get updated results); 'SUMIF' function on other hand works on real-time basis (changes in data instantly updates this formula) Syntax of the Sum IF function is as follows:

Example of the Sum IF function:

Given data is of quantities of fruits sale with summary of total quantities (kgs.) sold. To check the summary calculation, the SUMIF function can be easily used. Say for fruit-Dates, we take sum" of Col-D only for the records where 'Dates" appear in Col-

C. Therefore criteria range will be the Fruit-name (C19:C40), Criteria = C45 ("Dates") and sum range is quantities in Col D (D19:D40). It needs to be noted that the criteria range (19:40) matches with sum range (19:40). The calculated numbers can be compared with the given quantities to show the differences.



The 'VLOOKUP' Function

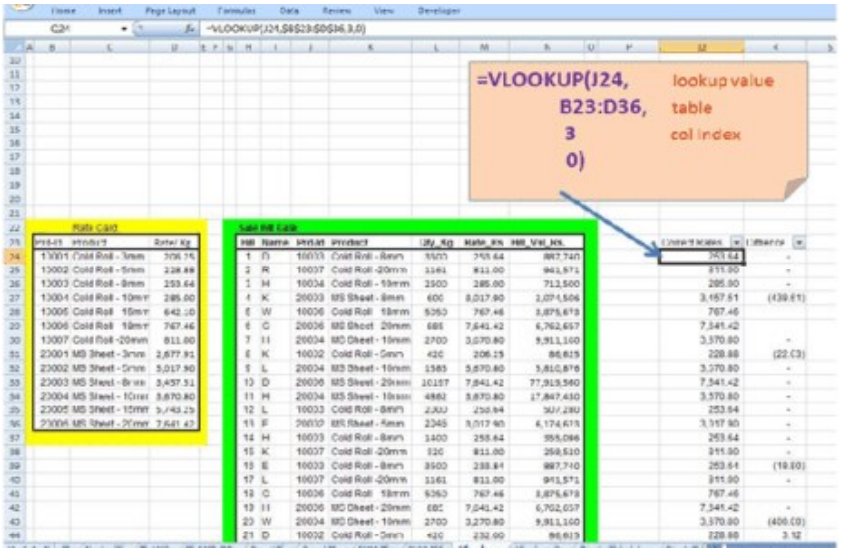
This function is extremely useful in linking two databases. This can be however, only done if there is a common unique reference (generally referred to as' primary key') between the two databases. All databases built-up on RDBMS work on this prime principle and hence generally it is easy to generate a primary key. There can be several applications of 'V Lookup' function. A few examples could be:

- To verify the rates billed with standard rate-card prices,
- To confirm proper application of interest rates charged for bank advances.
- To vouchsafe whether all dispatches are billed or vice-versa. Similarly vendor-bills can be checked with the Inventory receipts.

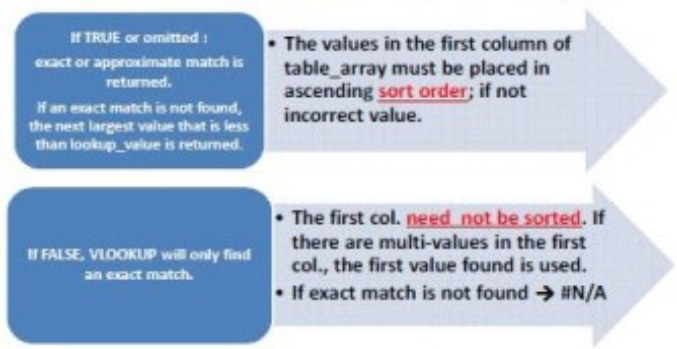
- Quantities, rates, etc. in purchase orders can be compared with the vendor bills. Or even the rates charged can be analyzed by comparing multi- vendors or same vendor over different period.
- Multi-years Inventories records can be compared.
- Employee payroll can be compared over the period or with master records.
- Tax rates for employees (withholding tax) , invoices, etc. can bechecked.
- Production records can be checked to inventories and vice-versa.
- The list can be endless and an effective use can be made depending upon the circumstances and subject matter of the audit / investigation.

Example of VLOOKUP

Given two databases (i) data of sales (marked with green frame) and (ii) data of standard rate card prices (marked with yellow frame). In practice usually the databases are in different worksheets or workbooks, but here it is shown in same worksheet for easy understanding. However the principle is same. The objective is to check whether the correct rates are invoiced to the customer. Using VLOOKUP function, the rates (in Col. D) of rate card (B23:D36) is extracted in Col-Q. The formula is explained in figure below. The difference between rates invoiced (Col. M) and rates chargeable (Col-Q extracted as aforesaid) can be compared.



The Col-R can be filtered for non-zero to list the differences which is list where the rates are charged higher or lower for further investigation.



This function quickly summarizes large data by:

- Querying the data in many user-friendly ways.
- Subtotaling and aggregating numeric data, summarizing data by categories, and subcategories, and creating custom calculations and formulae. Besides summing (sum), it can also find average, max, min, etc.
- Expanding and collapsing levels to focus on results, drilldowns to details from the summary
- Moving rows to columns or vice-versa; see different summaries using various scenarios.
- Filtering, sorting, grouping, etc.

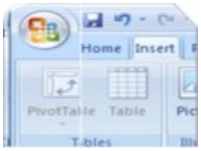
Application of Pivot Table function:

There can be several uses of the Pivot table function, a few examples can be as follows :

- Stratification / Classification of Data – period-wise, party-wise, assets-wise, etc.
- Creating various scenarios with if-then categories, using with filters it is possible to expand and collapse levels. For example in data of vendor bills, a pivot can be created to see Vendor-wise +Item_wise summary or Item-wise + Vendor_ wise summary.
- Create Trial Balance of General Ledger, Accounts Payable, Accounts Receivable, Bank Account balances, etc.
- Inventory Summary, Slow Moving / Non-moving Stock, etc.
- Digital Analysis e.g. Benfords Law, Relative Size Factor (RSF), etc.
- How to apply the Pivot Table.

Unlike many formulae, the Pivot function does not begin with a '=' sign. This is more of a command and hence not a formula. Therefore this command needs to refresh from time to

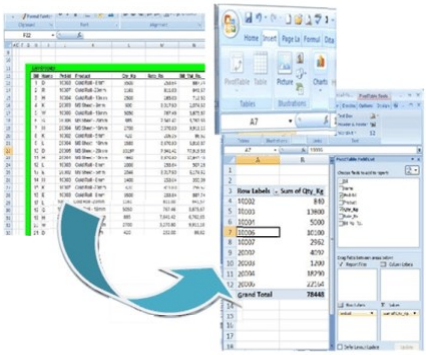
time to obtain correct results. If there is need for an update on real-time basis, one can use SUMIF, COUNTIF, etc.



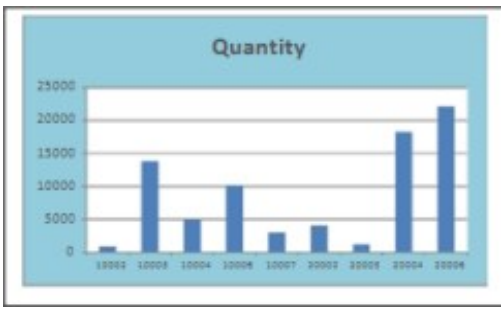
To apply the Pivot command, in the insert tab select the PivotTable icon and one needs to navigate throughthe interactive dialogue box. Select the appropriate data range and where you need to place the output (the appropriate choice generally should be 'in new sheet' since that will not conflict with your data).Select the appropriatefields for the vertical andhorizontal crosstabs as Rowlabels and Column labels. The data to be summarized should be placed in the 'value' section. Here by selecting the 'value field settings', one can select the sum, count, average, max, min, product, etc.Cosmetic touch can be given to the table by selecting appropriate formats or charts.

Example of Pivot Table:

Given data is of sales during a period giving details of Bill No., Customer name, Product_Id, Quantity billed, etc. The objective is to summarize the quantity product code wise. Applying the Pivot Table the pivot table / charts can be obtained as shown below:



In principle however complex queries and charts can be generated for different scenarios to give much more insights into the data.



Formula Auditing

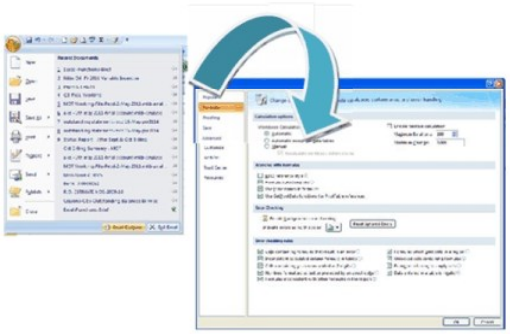
Very often some excel sheets are very complicatedly built-up -- there are many variables spread across multiple sheets and complex formulae make it difficult to audit. Most often such sheets are verified based on rebuild-and-compare method. This can sometime take enormous effort and hence may not be viable. This is where the Formula Auditing options come handy.

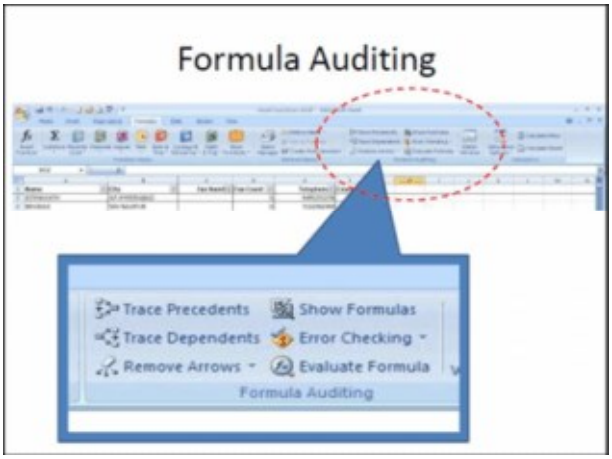
This is an in-built tool in MSExcel to quickly spot errors / omissions by locating inconsistencies in data having regard to surrounding region. A check run is conducted for:

- Cell containing formula that result in error
- Inconsistent calculated column in tables
- Cell containing years represented as two digits
- Numbers formatted as text
- Formulae inconsistent with other formulae in the region
- Formulae which omitted cells in a region
- Unlock cells containing formulae
- Formulae referring to empty cells
- Data entered in a table is invalid

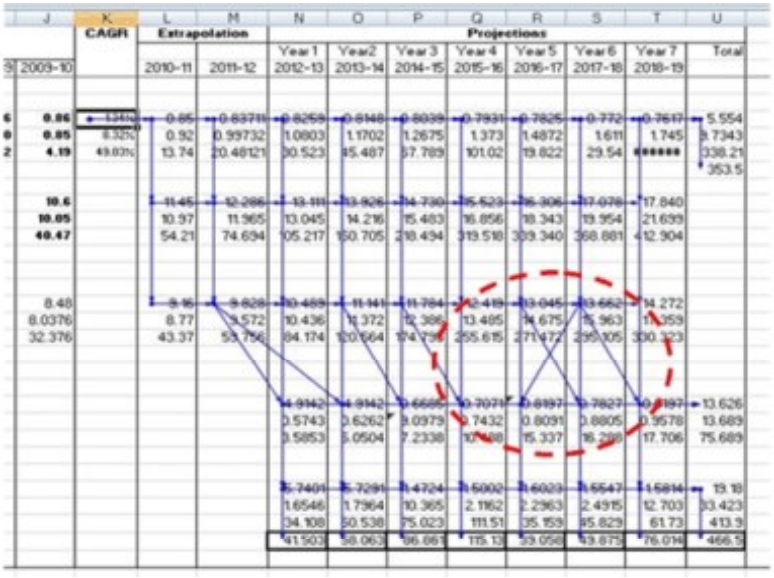
How to use the Formula Auditing Options

- Click on the 'Formula' tab and then select the 'Formula Auditing' section as shown in figure below. There are different audit tools available, a combination of which can throw up exceptions. Since this does not change the data, there no fear for data modification.

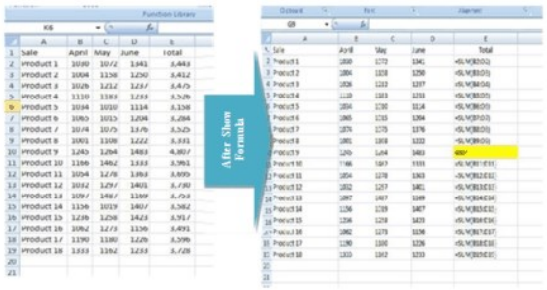




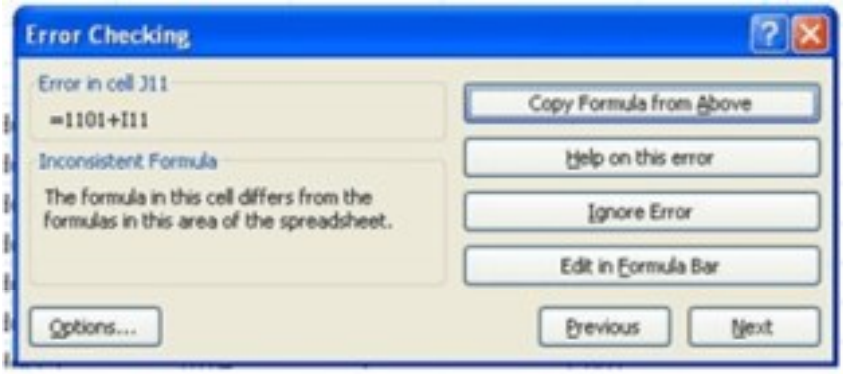
- Trace dependent and precedents diagrammatically show various relationship between the cells. Repeatedly pressing these commands shows a pattern of linkages (see the linkages in blue arrows in the figure below); one can easily spot variations (marked in red circle) if any.



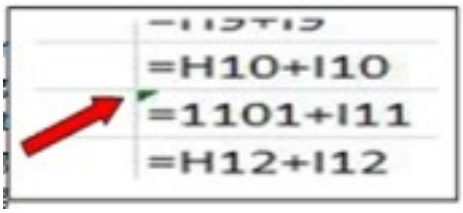
- As the name suggests, the 'Show Formula' tab quickly converts the entire sheet from value to the formula as shown below so that one can spot any glaring errors, e.g. direct numbers entered (see the yellow highlighted cell in fig. below) as against expected formula or vice versa, some extra numbers inserted in cell along with formulae, etc.



- Error checking commands works like a spell-check command. It basically checks all the possible errors and shows the errors in a dialogue box (as shown below) giving the cell numbers with possible error and explanation. The user can then correct the errors as he deems fit.



- Also one can use the green-corner sign (see adjacent screen shot) to spot errors. This is similar to the error checking. In error checking explanation is given, while in green-corner is just flagged (this is like the red line shown from wrong spelling in word file). This can be done by enabling the configuration settings in the as shown below.



Chapter 10
How to Write a Forensic Audit Report

"A Report is a statement of collected & considered facts, so drawn up as to give clear and concise information to persons who are not already in possession of the full facts of the subject matter of the report."

The Forensic Audit Report is nothing but statements of observation gathered & considered while proving conclusive evidence. It is a medium through which an auditors expresses his opinion under audit. It is an important part of the audit as it provides the results of the audit conducted by the auditor.

Points to Remember:

- Clear thinking :
  - ✓ To whom the report is directed
  - ✓ Purpose and aim
  - ✓ Cool and calm thinking to have logical and coherent presentation
  - ✓ Pattern of presentation
- Keep the reader uppermost in mind
  - ✓ Translate technical matters to layman's language
  - ✓ To visualize the reader's viewpoint
- Unbiased approach
  - ✓ To mention the view point of the auditee
- Impact of the report
  - ✓ What be the probable reaction to reporting whether action or decision will follow in quickest possible time or to be treated as of academic interest only.
  - ✓ To remember the universal saying – "don't jump to conclusions"
- Facts and figures to be in proper sequences

The main factors to go into the consideration for the various ways of presentations of written reports are:-

- Nature of business of the organization
- Nature of subject or aspect appraised

- For whom the report is intended
- Purpose for which the report is prepared
- Management attitude, directives and needs.
- Forensic auditor's approach and caliber.
- Extent of details required by auditee and management

A sample Table of Contents of a Forensic Audit Report may include the following:

1. EXECUTIVE SUMMARY

1.0 Background

1.1 Origin of the Audit

1.2 Audit Objective

1.3 Proposed Audit Outputs

1.4 Audit Implementation Approach

2. RISK ANALYSIS

2.1 Internal Environment Risk

2.1.1 Financial Management

2.1.2 Customers, Products and Competitors

2.1.3 Information technology

2.1.4 Business Process

2.1.5 Human Resource Management

2.2 External Environment Forces

2.2.1 Influence of Economics and relevant Market

2.2.2 Political and Legal Scenario

2.2.3 Technology in the Sector

3. AUDIT PROCESS

3.1. Preliminary understanding of scope and incident coverage

(i) Identification of all related data elements

(ii) Preparation of a List of "persons of interest" for interview

(iii) Obtain management approval for scope

3.2. Collect Evidence

Chapter 11
Digital Forensics

Digital forensics has been defined as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations. It is the application of proven scientific methods and techniques in order to recover data from electronic / digital media. Digital Forensic specialists work in the field as well as in the lab.

In the early 1980s personal computers became more accessible to consumers, leading to their increased use in criminal activity (for example, to help commit fraud). At the same time, several new "computer crimes" were recognized (such as hacking). The discipline of computer forensics emerged during this time as a method to recover and investigate digital evidence for use in court. A computer forensic investigator follows certain stages and procedures when working on a case. First he identifies the crime, along with the computer and other tools used to commit the crime. Then he gathers evidence and builds a suitable chain of custody. The investigator must follow these procedures as thoroughly as possible. Once he recovers data, he must image, duplicate, and replicate it, and then analyze the duplicated evidence. After the evidence has been analyzed, the investigator must act as an expert witness and present the evidence in court. The investigator becomes the tool which law enforcement uses to track and prosecute cyber criminals. Forensic investigator follows all of these steps and that the process contains no misinformation that could ruin his reputation or the reputation of an organization.

Stages of Forensic Investigation in Digital forensics includes Assessing, preserving, collecting, confirming, identifying, analyzing, recording, and presenting crime scene information.

1. Assess the Crime scene

To conduct a computer investigation, first one need to obtain proper authorization. That process begins with the step of assessing the case, asking people questions, and documenting the results in an effort to identify the crime and the location of the evidence. Review the organization’s policies and laws and build a team for the investigation.In this investigators prioritize the actions and justify the resources for the internal investigation.

2. Collection phase

The first step in the forensic process is to identify potential sources of data and acquire forensic data from them. Major sources of data are desktops, storage media, Routers, Cell Phones, Digital Camera etc. A plan is developed to acquire data according to their importance, volatility and amount of effort to collect

Evidence is most commonly found in files and Databases that are stored on hard drives and storage devices and media. Finding the evidence, discovering relevant data, preparing an Order of Volatility, eradicating external avenues of alteration, gathering the evidence, and preparing a chain of custody are the main steps in the collection phase. Maintaining the chain of custody is the important step. Identification of the evidence must be preserved to maintain its integrity.

3. Analysis phase

This involves examining the collected data/files and finding out the actual evidence. The computer forensic investigator must trace, filter, and extract hidden data during the process.

4. Report phase

The audience will be able to understand the evidence data which has been acquired from the evidence collection and analysis phases. The report generation phase records the evidence data found out by each analysis component. Additionally, it records the time and provides hash values of the collected evidence for the chain-of-custody.

Chain-of-custody and Documentation

Documentation is essential to the investigation. For evidence to be reliable in court, integrity has to be preserved. Safe storage and tamper protection is needed, so is also the documenting of handling, i.e. who has accessed the evidence while it was in custody. Chain of custody prevents accusation in court that the evidence has been tempered with. Evidence need to be identified and labelled as soon as it is collected. All actions performed by the investigator should be documented, including the reasons for doing so. In digital forensics, this means logging all actions and integrity checks.

11.1 Types of Digital Evidence

- PERSISTANT DATA - Meaning data that remains intact when the computer is turned off. E.g. hard drives, disk drives and removable storage devices (such as USB drives or flash drives).
- VOLATILE DATA - Which is data that would be lost if the computer is turned off. E.g. deleted files, computer history, the computer's registry, temporary files and web browsing history.

11.2 Top 10 Locations for Evidence

- Internet History Files
- Temporary Internet Files
- Slack/Unallocated Space
- Buddy lists, personal chat room records, P2P, others saved areas

- News groups/club lists/posting
- Settings, folder structure, file names
- File Storage Dates
- Software/Hardware added
- File Sharing ability
- E-mails

11.3 Computer Forensics Methodology

- Shut Down the Computer
- Document the Hardware Configuration of The System
- Transport the Computer System to A Secure Location
- Make Bit Stream Backups of Hard Disks and Floppy Disks
- Mathematically Verify Data on All Storage Devices
- Document the System Date and Time
- Make a List of Key Search Words
- Evaluate the Windows Swap File
- Evaluate File Slack
- Evaluate Unallocated Space (Erased Files)
- Search Files, File Slack and Unallocated Space for Key Words
- Document File Names, Dates and Times
- Identify File, Program and Storage Anomalies
- Evaluate Program Functionality
- Document Your Findings

Chapter 12
Cyber Crime

- Computer or computer networks are used as a tool or a target or a place of criminal activity
- First recorded Cyber Crime took place in the year 1820 in France.
- Unauthorized access to computer system, data destruction, data alteration, theft of intellectual property.
- Most important revenue sector for global organized crime
- Easy to learn how to commit
- Require few resources relative to potential damage caused
- Can be committed in a jurisdiction without being physically present in it
- Are often not clearly illegal
- Problematical
- Any crime where computer is a tool, target or both
- Offences against computer data / systems
- Unauthorized access, modification or impairment of a computer or digital system
- Offences against the confidentiality, integrity and availability of computer data or systems

The first recorded cyber-crime took place in 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest from of a computer, has been around since 3500 B.C.

In India, Japan and China, the era of modern computer, however, began with the analytical engine of Charles Babbage. The first spam email took place in 1978 when it was sent out over the ARPANT. The first virus was installed on an Apple computer in 1982 when a high school student, Rich Skrenta, developed the EIK Cloner.

Categories of Cyber Crime

We can categorize cyber-crime in two ways

- The computer as a target: - using a computer to attacks other computer, e.g. Hacking, virus/worms attacks, Dos attack etc.

- The computer as a weapon: - using a computer to commit real world crime e.g. cyber terrorism, credit card fraud and pornography etc.

Types of Cyber Crime

HACKING: Hacking, in simple terms means illegal intrusion of information non a computer system and /or network. Government websites are the hot target soft he hackers due to the press coverage it receives. Hackers enjoy the media coverage. Motive behind such crimes are greed, power, publicity, revenge, adventure, desire to access for bidden information etc.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(a) read with section 66 is applicable and Section 379 & 406 of Indian Penal Code, 1860 also are applicable. If crime is proved under IT Act, accused shall be punished for imprisonment, which may extend to three years or with fine, which may extend to five lakh rupees or both. Hacking offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate

DATA THEFT: Data theft is growing problem, primarily perpetrated by office workers with access of technology such computers, laptops and hand-held devices, capable of storing digital information such as flash drives, iPods and even digital cameras. The damage caused by data theft can be considerable with today's ability to transmit very large files via e-mail, web pages, USB devices, DVD storage and other hand-held devices. According to Information Technology (Amendment) Act, 2008, crime of data theft under Section 43 (b) is stated as - If any person without permission of the owner or any other person, who is in charge of a computer, computer system of computer network - downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium, then it is data theft.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(b) read with Section 66 is applicable and under Section 379, 405 & 420 of Indian Penal Code, 1860 also applicable. Data Theft offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

E-MAIL SPOOFING: E-mail spoofing is e-mail activity in which the sender addresses and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is sending an e-mail to another person in such a way that it appears that the e-mail was sent by someone else. A spoof email is one that appears to originate from one source but actually has been sent from another source. Spoofing is the act of electronically disguising one computer as another for gaining as the password system. It is becoming so common that you can no longer take for granted that the e-mail you are receiving is truly from the person identified as the sender.

Email spoofing is a technique used by hackers to fraudulently send email messages in which the sender address and other parts of the email header are altered to appear as though the email originated from a source other than its actual source. Hackers use this method to disguise the actual email address from which phishing and spam messages are sent and often use email spoofing in conjunction with Web page spoofing to trick users into providing personal and confidential information.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 66-D and Section417, 419 & 465of Indian Penal Code, 1860 also applicable. Email spoofing offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

IDENTITY THEFT : Identity theft is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. Information Technology (Amendment) Act, 2008, crime of identity theft under Section 66-C, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person known as identity theft.

Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can suffer various consequences when they are held responsible for the perpetrator's actions. At one time the only way for someone to steal somebody else's identity was by killing that person and taking his place. It was typically a violent crime. However, since then, the crime has evolved and today's white collared criminals are a lot less brutal. But the ramifications of an identity theft are still scary.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 66-C and Section 419 of Indian Penal Code, 1860 also applicable. Identity Theft offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

CHILD PORNOGRAPHY: The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. As more homes have access to internet, more children would be using the internet and more are the chances of falling victim to the aggression of Pedophiles.

How Do They Operate: How do they operate Pedophiles use false identity to trap the children, Pedophiles connect children in various chat rooms which are used by children to interact with other children.

DENIAL OF SERVICE ATTACKS: This is an act by the criminals who floods the bandwidth of the victim's network or fills his E-mail box with spam mail depriving him of the service he is entitled to access or provide. Many DOS attacks, such as the ping of death and Tear drop attacks.

VIRUS DISSEMINATION: Malicious software that attaches itself to other software. VIRUS, WORMS, TROJAN HORSE,WEB JACKING, E-MAIL BOMBING etc.

COMPUTER VANDALISM: Damaging or destroying data rather than stealing or misusing them is called cyber vandalism. These are program that attach themselves to a file and then circulate.

CYBER TERRORISM: Terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate E-mails, attacks on service network etc.

SOFTWARE PIRACY: Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

Chapter 13
Applicable Laws– India

- The Information Technology Act, 2000
- Indian Penal code 1860
- Civil Procedure Code 1908
- Indian Contract Act, 1872
- Indian Evidence Act, 1872
- The Prevention of Money Laundering Act, 2002
- The Foreign Exchange Management Act, 1999
- The Companies Act, 2013
- RBI - Master Circular on Frauds- Classification and Reporting

13.1 The Information Technology Act, 2000, Amended 2008

The IT Act recognizes offences related to fraud such as tampering with computer source documents, hacking computer systems, creating, publishing, or otherwise making available digital signature for any fraudulent purpose. The Act also provides legitimacy to electronic records and approvals and recognizes the evidential value electronic records, emails and electronic approvals and allows them to be used instead of paper documents subject to them meeting the guidelines provided in the Act.

The intent of the Act is to provide legal recognition for the transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "Electronic Commerce", which involve the use of alternatives to paper based methods of communication and storage of information , to facilitate electronic filings of documents with the Government agencies and further to amend the Indian Penal Code, Indian Evidence Act, 1872,, The Bankers' Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

The Act brings focus to digital signatures and data privacy as well as defines the use of intermediaries and sets up a structure to ensure compliance. A copy of the Act is provided as part of the material for this course and the candidates would be well advised to review and familiarize themselves with the content.

The Act also sets up Indian Computer Emergency Response Team to serve as national agency for incident response which shall serve as the national agency for performing the following functions in the area of Cyber Security,-

(a) Collection, analysis and dissemination of information on cyber incidents

(b) Forecast and alerts of cyber security incidents

(c) Emergency measures for handling cyber security incidents

(d) Coordination of cyber incidents response activities

(e) Issue guidelines, advisories, vulnerability notes and white papers relating to Information security practices, procedures, prevention, response and reporting of Cyber incidents

(e) Such other functions relating to cyber security as may be prescribed

(f) The fraud related offences and their relevant punishments included in the IT Act are as follows:

Section No.	Nature of Offense	Penalty and /or Fine
65	Tampering with the computer source documents	**Penalties:** Imprisonment up to 3 years and / or **Fine:** Two lakh rupees.
66	Hacking with computer system	**Penalties:** Punishment: Imprisoned up to three years and **Fine:** which may extend up to two lakh rupees or with both.
67	Publishing of information which is obscene in electronic form	**Penalties:** Punishment: (1) On first conviction --- imprisonment which may extend up to five years. **Fine:** up to on first conviction which may extend to one lakh rupees. (2) On second conviction ---- imprisonment up to which may extend to ten years and Fine which may extend up to two lakh rupees.
71	Misrepresentation	**Penalties:** Punishment: imprisonment which may extend to two years **Fine:** may extend to one lakh rupees or with both.
72	Breach of confidentiality and privacy	**Penalties:** Punishment: term which may extend to two years. **Fine:** one lakh rupees or with both.
73	Publishing false Digital Signature Certificate	**Penalties:** Punishment imprisonment of a term of which may extend to two years. **Fine:** fine may extend to 1 lakh rupees or with both.
74	Publication for fraudulent purpose	Punishment: imprisonment for a term up to two years. **Fine:** up to one lakh or both.

13.2 Indian Penal Code 1860

Indian Penal Code is the main criminal code of India. It is a comprehensive code intended to cover all substantive aspects of criminal law.

There is no separate legislation dealing with fraud as in the United Kingdom or the USA. Fraudulent activities are covered by the Indian Penal Code. The word 'fraud' is not defined in Indian Penal Code; instead what constitutes doing a thing fraudulently is explained. Section 25 defines the expression 'fraudulently' – 'a person is said to do a thing fraudulently if he does that with intent to defraud but not otherwise'. The expression fraudulently occurs in Sections 206, 207, 208, 242, 246, 247, 252, 253, 261, 262, 263 and Sections 421 to 424.

Sections 24 and 23 define expressions 'dishonestly' and 'wrongful gain and wrongful loss. 'Wrongful gain' is gain by unlawful means of property which the person gaining is not legally entitled. 'Wrongful loss' is the loss by unlawful means of property to which the person losing it is legally entitled. Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing 'dishonestly'.

Indian Penal Code recognizes the following acts as fraud:

(a) Impersonation

(b) Counterfeiting

(c) Wrong weighing and measurement

(d) Misappropriation

(e) Criminal breach of trust

(f) Cheating

(g) Dishonest dealing in property

(h) Mischief

(i) Forgery

(j) Falsification

(k) Possessing stolen property

(l) Concealment

(m) Some of the important provisions of the IPC in this regard are discussed hereunder-

(n) **(a) Section 403 of IPC-Dishonest misappropriation of property:** According to this provision, whoever dishonestly misappropriates or convert to his own use, any movable property, shall be punished with imprisonment for a term which may extend to two years or with fine or with both.

(o) For example, A takes B's property in good faith believing that the property belongs to

himself. A is not guilty of misappropriation. But even after discovering his mistake, A dishonestly misappropriates the property to his own use, he is guilty of an offence under this section.

(p) Explanation 1 to the section states that a dishonest misappropriation for the time being only is a misappropriation within the meaning of this section. For example, A finds a property and takes it with the intention of restoring it to the owner, A is not guilty of offence. But if he appropriates it for his own use without using reasonable means to discover the owner, he is guilty of the offence.

(q) **(b) Section 405 of IPC-Criminal breach of trust:** According to this provision, anybody entrusted with the property dishonestly misappropriates or converts to his own use or dishonestly uses or disposes of that property in violation of any 3 direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, which he has made touching the discharging of such trust, commits criminal breach of trust.

(r) For example, A, an executor of a will, dishonestly disobeys the law which directs him to divide the property according to the Will and appropriate the same to his own use, A has committed criminal breach of trust. Section 406 prescribes punishment for criminal breach of trust which is imprisonment extending to three years or fine or both. Section 409 of IPC prescribes higher imprisonment of upto ten years in respect of criminal breach of trust by a public servant or by a banker or merchant or agent.

(s) **(c) Section 415 of IPC –Cheating :** According to this provision, whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property, to any person, or to consent that any person shall retain any property or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit, if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, reputation or property, commits cheating. Examples: (a) A, by falsely pretending to be in civil service, intentionally deceives B and thus dishonestly induces B to let him have on credit goods for which he does not mean to pay, A cheats. (b) A, by putting a counterfeit mark on an article, intentionally deceives B into a belief that this article was made by a certain celebrated manufacturer, and thus dishonestly induces B to buy and pay for the article, A cheats.

(t) **(d) Section 463-Forgery:** It is defined as- " Whoever makes any false document or false electronic record or, part of a document, or electronic record, with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery". 4 The Madras High Court in AIR 1968 Mad 349 held that in order to constitute an offence under this section, the document must be false and it must have been made dishonestly or fraudulently and it must have been made with one of the intention specified in section

463. In AIR 1979 SC 1890, Supreme Court held that mere presenting a lottery ticket to the state authority which later on was detected as a forged one does not by itself amount to forgery. The knowledge of forged document is a necessary requirement. Section 465 prescribes a punishment for forgery which is imprisonment for a term which may extend to two years or with fine or with both.

13.3 Civil Procedure Code 1908

Civil procedure is the body of law that sets out the rules and standards that courts follow when adjudicating civil lawsuits (as opposed to procedures in criminal law matters). These rules govern how a lawsuit or case may be commenced, what kind of service of process (if any) is required, the types of pleadings or statements of case, motions or applications, and orders allowed in civil cases, the timing and manner of depositions and discovery or disclosure, the conduct of trials, the process for judgment, various available remedies, and how the courts and clerks must function.

13.4 Indian Contract Act, 1872

Under the Indian Contract Act, 1872, Sec.17 defines fraud.

"Fraud means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agents, with intent to deceive another party thereto his agent, or to induce him to enter into the contract;

(1) The suggestion as a fact, of that which is not true, by one who does not believe it to be true;

(2) The active concealment of a fact by one having knowledge or belief of the fact;

(3) A promise made without any intention of performing it;

(4) Any other act fitted to deceive;

(5) Any such act or omission as the law specially declares to be fraudulent.

Explanation.—Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak, or unless his silence, is, in itself, equivalent to speech."

Section 19 'Voidability of agreement without free consent' states *'When consent to an agreement is caused by coercion, fraud or misrepresentation, the agreement is a contract voidable at the option of the party whose consent was so caused';*

'A party to a contract whose consent was caused by fraud or misrepresentation, may, if he thinks fit, insist that the contract hall be performed and that he shall be put in the position in which he would have been if the representations made had been true.'

Hence the section seeks to provide protection to the defrauded party as the contract which is

entered into by fraud is voidable at the option of the defrauded contracting party. Further it also grants the defrauded party an option in form of a right of enforcement of the contract and indemnity against the loss caused to him on account of such fraud which he would not have been subject to had the contact been entered into by proper representation.

The only cases which are outside the purview of section 19 are those in which the defrauded party could have obtained the knowledge of fraud by due diligence and where he failed to apply such due diligence.

13.5 Indian Evidence Act, 1872

The Indian Evidence Act, originally passed by the Imperial Legislative Council in 1872, during the British Raj, contains a set of rules and allied issues governing admissibility of evidence in the Indian courts of law.

Section 44 in the Indian Evidence Act, 1872

Fraud or collusion in obtaining judgment, or incompetency of Court, may be proved.—Any party to a suit or other proceeding may show that any judgment, order or decree which is relevant under section 40, 41 or 42 and which has been proved by the adverse party, was delivered by a Court not competent to deliver it, or was obtained by fraud or collusion. tc "44. Fraud or collusion in obtaining judgment, or incompetency of Court, may be proved.—Any party to a suit or other proceeding may show that any judgment, order or decree which is relevant under section 40, 41 or 42 and which has been proved by the adverse party, was delivered by a Court not competent to deliver it, or was obtained by fraud or collusion."

13.6 The Prevention of Money Laundering Act, 2002

The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. PMLA and the Rules notified there under came into force with effect from July 1, 2005. Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant sections of the Act to implement the provisions of the Act.

The PMLA and rules notified there under impose obligation on banking companies, financial institutions and intermediaries to verify identity of clients, maintain records and furnish information to FIU-IND. PMLA defines money laundering offence and provides for the freezing, seizure and confiscation of the proceeds of crime.

PMLA empowers certain officers of the Directorate of Enforcement to carry out investigations in cases involving offence of money laundering and also to attach the property involved in money laundering. PMLA envisages setting up of an Adjudicating Authority to exercise jurisdiction, power and authority conferred by it essentially to confirm attachment or order confiscation of attached properties. It also envisages setting up of an Appellate Tribunal to hear appeals against the order of the Adjudicating Authority and the authorities like Director FIU-IND.

13.7 The Foreign Exchange Management Act, 1999

The Foreign Exchange Management Act, 1999 (FEMA) is an Act of the Parliament of India "to consolidate and amend the law relating to foreign exchange with the objective of facilitating external trade and payments and for promoting the orderly development and maintenance of foreign exchange market in India". It was passed in the winter session of Parliament in 1999, replacing the Foreign Exchange Regulation Act (FERA). This act seeks to make offenses related to foreign exchange civil offenses. It extends to the whole of India. It enabled a new foreign exchange management regime consistent with the emerging framework of the World Trade Organization (WTO). It also paved way to Prevention of Money Laundering Act 2002, which was effected from 1 July 2005.

FEMA permits only authorized person to deal in foreign exchange or foreign security. Such an authorized person, under the Act, means authorized dealer, money changer, off-shore banking unit or any other person for the time being authorized by Reserve Bank. The Act thus prohibits any person who:-

- Deal in or transfer any foreign exchange or foreign security to any person not being an authorized person;
- Make any payment to or for the credit of any person resident outside India in any manner;
- Receive otherwise through an authorized person, any payment by order or on behalf of any person resident outside India in any manner;
- Enter into any financial transaction in India as consideration for or in association with acquisition or creation or transfer of a right to acquire, any asset outside India by any person is resident in India which acquire, hold, own, possess or transfer any foreign exchange, foreign security or any immovable property situated outside India.

Main Features

- Activities such as payments made to any person outside India or receipts from them, along with the deals in foreign exchange and foreign security is restricted. It is FEMA that gives the central government the power to impose the restrictions.
- Restrictions are imposed on residents of India who carry out transactions in foreign exchange, foreign security or who own or hold immovable property abroad.
- Without general or specific permission of the MA restricts the transactions involving foreign exchange or foreign security and payments from outside the country to India – the transactions should be made only through an authorised person.
- Deals in foreign exchange under the current account by an authorised person can be restricted by the Central Government, based on public interest.
- Although selling or drawing of foreign exchange is done through an authorized person,

the RBI is empowered by this Act to subject the capital account transactions to a number of restrictions.

- Residents of India will be permitted to carry out transactions in foreign exchange, foreign security or to own or hold immovable property abroad if the currency, security or property was owned or acquired when he/she was living outside India, or when it was inherited by him/her from someone living outside India.
- Exporters are needed to furnish their export details to RBI. To ensure that the transactions are carried out properly, RBI may ask the exporters to comply with its necessary requirements.

13.8 The Companies Act, 2013

Comprehensive explanation of term Fraud is given in Explanation to Section 447(1) of The Companies Act, 2013 as follows:

"Fraud" in relation to affairs of a company or any body corporate, includes

(a) Any act,

(b) Omission,

(c) Concealment of any fact or

(d) Abuse of position committed by any person or any other person with the connivance in any manner, -

- with intent to deceive,
- to gain undue advantage from, or
- to injure the interests of,
    - o the company or
    - o its shareholders or
    - o its creditors or
    - o any other person,

Whether or not there is any wrongful gain or wrongful loss;

- "Wrongful gain" means the gain by unlawful means of property to which the person gaining is not legally entitled;
- "Wrongful loss" means the loss by unlawful means of property to which the person losing is legally entitled.

Statutory provisions of Fraud and Fraud Reporting under The Companies Act, 2013

Section 447 of the Companies Act, 2013 often now referred as one of the draconian section of

the new Act deals with provision relating to punishment for fraud. It reads as: "Without prejudice to any liability including repayment of any debt under this Act or any other law for the time being in force, any person who is found to be guilty of fraud, shall be punishable with imprisonment for a term which shall not be less than 6 months but which may extend to 10 years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extend to 3 times the amount involved in the fraud.

Where the fraud in question involves public interest, the term of imprisonment shall not be less than 3 years".

The Companies Act, 2013 has provided punishment for fraud as provided under section 447 in around 20 sections of the Act e.g. u/s 7(5), 7(6), 8(11), 34, 36, 38(1), 46(5), 56(7), 66(10), 75, 140(5), 206(4), 213, 229, 251(1), 266(1), 339(3), 448 etc. for directors, key managerial personnel, auditors and/or officers of company. Thus, the new Act goes beyond professional liability for fraud and extends to personal liability if a company contravenes such provisions.

Under section 140 the auditors and their firm would be jointly liable for any frauds in the books of accounts and many auditors are likely to become forensic accountants in the days to come to avoid being caught on the wrong foot.

The Companies Act, 2013 via Section 143 has cast a responsibility of reporting the Frauds to the Central Government on the Auditors.

Who has to Report?

1. The Statutory Auditor including Joint Auditor , and also the Auditor in the course of providing attest services like
   (a) Clause 41 of the Listing Agreement with Stock Exchanges requires the statutory auditor to perform limited review/audit of the quarterly financial results published by the listed companies
   (b) the auditor may also be engaged by the Board of directors of the company to carry out the audit of interim financial statements prepared by the management as per Accounting Standard 25 and report on such interim financial statements to the Board of Directors
   (c) the auditor may also perform Tax Audit under the Income-tax Act
   (d) the auditor may be engaged to issue certificates
2. The Cost Accountant conducting cost audit under Section 148 of the Act
3. The Company Secretary in practice, conducting secretarial audit under Section 204 of the Act,
4. The Branch Auditors appointed under Section 139 of the Act with respect to the branch.

What Frauds need to be reported?

Section 143 includes only fraud by officers or employees of the company and does not include fraud by third parties such as vendors and customers. The fraud needs to be reported **only if** the auditor is the first person to identify/note such fraud. In case a fraud has already been reported or has been identified/detected by the management or through the company's vigil/whistle blower mechanism and has been/is being remediated/dealt with by them and such case is informed to the auditor, he will not be required to report the same.

The Companies Act, 2013 has included a comprehensive definition of fraud and stringent provisions regarding punishment for such frauds. Moreover, independent professionals shall also be held liable for action and proceeded against under the Act.

Section 447 of the Companies Act now referred to as the draconian section which deals with provisions relating to punishment for fraud.

What is the penalty for violation?

I. **Imprisonment:** [6 months to 10 years] & In cases where fraud involves public interest, term of imprisonment not to be less than 3 years

II. **Fine:** Not less than amount involved in the fraud and extending to three times the amount in certain casesThe below table includes certain sections that attract liability u/s 447 of the Companies Act. These are cognizable offences and the person accused of any such offense shall not be released on bail or on his or her own bond, unless subject to exception provided /s 212(6)

Section	Fraud w.r.t.	Who will be penalized
7(5)	Registration of a company	A person furnishing false information or suppressing any material information of which he or she is aware
36	Inducing persons to invest money	The person doing so
75(1)	Acceptance of deposit with intent to defraud depositors or for any fraudulent purpose	Every officer of the company who accepted deposit
206(4)	Conducting business of a company for a fraudulent or unlawful purpose	Every officer of the company who is in default
213	**OTHER CASES** ➢ Business of a company being conducted with intent to defraud its creditors ➢ Fraud, misfeasance or other misconduct of the company or any of its members, or	Every officer of the company who is in default and the person(s) concerned in the formation of the company or management of its affairs

	➢ Company withholding information from members with respect to its affairs, which they may reasonably expect	
229	Furnishing false statement or mutilation or destruction of documents	Person required to provide an explanation or make a statement during the course of inspection, inquiry or investigation, or the officer or other employee as required
251(1)	Application for removal of name from register with the object of evading liabilities/intent to deceive	Persons in charge of management of the company
339(3)	Conducting business of company with intent to defraud its creditors, any other persons or for any fraudulent purpose	Every person who was knowingly a party to the business in the aforesaid manner
448	Making a false statement in any return, report, certificate, financial statements or other document required by or for the purpose of any of the provisions of this Act or the rules made thereunder	Person making such a statement

Chapter 14
Applicable Laws – Outside India

I. Fraud Act, 2006 – United Kingdom

The Fraud Act came into force on the 15th January 2007. By introducing a general offence of "fraud", the aim was to simplify the law by replacing the various deception offences under the Theft Act, 1968. This new general offence of fraud is set out in section 1 of the Act. It can be committed in three ways:

- Fraud by false representation;
- Fraud by failing to disclose information;
- Fraud by abuse of position.

A person who is guilty of fraud is liable on conviction on indictment to imprisonment for a term not exceeding 10 years or to a fine (or both).

Each offence in the Fraud Act 2006 is a conduct offence, complete on the accused's acts notwithstanding any result caused. So there is no need to prove a result of any kind, it is sufficient that the person intends to cause loss or make a gain.

- "Fraud by false representation" is defined by Section 2 of the Act as a case where a person makes "any representation as to fact or law ... express or implied" which they know to be untrue or misleading.
- "Fraud by failing to disclose information" is defined by Section 3 of the Act as a case where a person fails to disclose any information to a third party when they are under a legal duty to disclose such information.
- "Fraud by abuse of position" is defined by Section 4 of the Act as a case where a person occupies a position where they are expected to safeguard the financial interests of another person, and abuses that position; this includes cases where the abuse consisted of an omission rather than an overt act.

In all three classes of fraud, it requires that for an offence to have occurred, the person must have acted dishonestly, and that they had to have acted with the intent of making a gain for themselves or anyone else, or inflicting a loss (or a risk of loss) on another.

A "gain" or a "loss" is defined to consist only of a gain or a loss in money or property (including intangible property), but could be temporary or permanent. A "gain" could be construed as gaining by keeping their existing possessions, not just by obtaining new ones, and loss included losses of expected acquisitions, as well as losses of already-held property.

The Act will establish two "supporting" offences, these being the possession of articles for use in frauds (Section 6) and the making or supplying of articles for use in frauds (Section 7).

Section 11 of the Act makes it a statutory offence to obtain services dishonestly; meaning that services which were to be paid for were obtained with the knowledge or intention that no payment would be made. A person found guilty of this will be liable to a fine or imprisonment for up to twelve months on summary conviction (six months in Northern Ireland), or a fine or imprisonment for up to five years on conviction on indictment.

In regard to the fraudulent behavior of companies, the existing offence of participating in fraudulent business carried on by a company, provided for by the Companies Act 1985, was amended by Section 10 - bringing the maximum penalty from 7 years imprisonment to 10 years [And/or a fine] - and a new offence of participating in fraudulent business carried on by a sole trader was established by Section 9.

Section 12 of the Act provides that where an offence against the Act was committed by a body corporate, but was carried out with the "consent or connivance" of any director, manager, secretary or officer of the body - or any person purporting to be such - then that person, as well as the body itself, is liable.

II. Bribery Act, 2010 – United Kingdom

The Bribery Act 2010 was introduced to update and enhance UK law on bribery including foreign bribery in order to address better the requirements of the 1997 OECD anti-bribery Convention. It is now among the strictest legislation internationally on bribery. Notably, it introduces a new strict liability offence for companies and partnerships of failing to prevent bribery.

The introduction of this new corporate criminal offence places a burden of proof on companies to show they have adequate procedures in place to prevent bribery. The Bribery Act also provides for strict penalties for active and passive bribery by individuals as well as companies.

The crime of bribery is described in Section 1 as occurring when a person offers, gives or promises to give a "financial or other advantage" to another individual in exchange for "improperly" performing a "relevant function or activity".

The Bribery Act creates four prime offences:

- Two general offences covering the offering, promising or giving of an advantage, and requesting, agreeing to receive or accepting of an advantage;
- A discrete offence of bribery of a foreign public official ; and
- A new offence of failure by a commercial organisation to prevent a bribe being paid to obtain or retain business or a business advantage (should an offence be committed, it will be a defence that the organisation has adequate procedures in place to prevent bribery).

The Bribery Act is legislation of great significance for companies incorporated in or carrying on business in the UK. It presents heightened liability risks for companies, directors and individuals. To avoid corporate liability for bribery, companies must make sure that they have strong, up-to-date and effective anti-bribery policies and systems.

The Bribery Act unlike previous legislation places strict liability upon companies for failure to prevent bribes being given (active bribery) and the only defence is that the company had in place adequate procedures designed to prevent persons associated with it from undertaking bribery.

The Bribery Act has extra-territorial reach both for UK companies operating abroad and for overseas companies with a presence in the UK.

UK companies doing business overseas -

Companies registered in the UK must take note of the extra-territorial reach of the Bribery Act. A company can commit an offence under section 7 of failure to prevent bribery if an employee, subsidiary, agent or service provider ('associated persons') bribes another person anywhere in the world to obtain or retain business or a business advantage.

A foreign subsidiary of a UK company can cause the parent company to become liable under section 7 when the subsidiary commits an act of bribery in the context of performing services for the UK parent. If the foreign subsidiary were acting entirely on its own account it would not cause the UK parent to be liable for failure to prevent bribery under section 7 as it would not then be performing services for the UK parent.

However, the UK parent might still be liable for the actions of its subsidiary in other ways such as false accounting offences or under the Proceeds of Crime Act 2002.

Foreign companies with operations in the UK -

The Bribery Act has important implications for foreign companies which do business in the UK as its territorial scope is extensive. The corporate offence set out in Section 7 of failure to prevent bribery in the course of business applies to any relevant commercial organization defined as a body incorporated under the law of the United Kingdom (or United Kingdom registered partnership) and any overseas entity that carries on a business or part of a business in the United Kingdom.

A foreign company which carries on any part of its business in the UK could be prosecuted for failure to prevent bribery even where the bribery takes place wholly outside the UK and the benefit or advantage to the company is intended to accrue outside the UK.

Section 11 explains the penalties for individuals and companies found guilty of committing a crime. If an individual is found guilty of a bribery offence, tried as a summary offence, they may be imprisoned for up to 12 months and fined up to £5,000. Someone found guilty on indictment, however, faces up to 10 years' imprisonment and an unlimited fine. The crime of a commercial organization failing to prevent bribery is punishable by an unlimited fine. In

addition, a convicted individual or organization may be subject to a confiscation order under the Proceeds of Crime Act 2002, while a company director who is convicted may be disqualified under the Company Directors Disqualification Act 1986.

(The Proceeds of Crime Act 2002 (c.29) (POCA) is an Act of the Parliament of the United Kingdom which provides for the confiscation or civil recovery of the proceeds from crime and contains the principal money laundering legislation in the UK.)

III. Foreign Corrupt Practices Act, 1977 – United States of America

The Foreign Corrupt Practices Act of 1977 (FCPA) is a United States federal law known primarily for two of its main provisions, one that addresses accounting transparency requirements under the Securities Exchange Act of 1934 and another concerning bribery of foreign officials.

The Act was signed into law by President Jimmy Carter on December 19, 1977, and amended in 1998 by the International Anti-Bribery Act of 1998 which was designed to implement the anti-bribery conventions of the Organization for Economic Co-operation and Development.

IV. OECD Anti-Bribery Convention

http://www.oecd.org/daf/anti-bribery/anti-briberyconvention/

The OECD Anti-Bribery Convention (officially Convention on Combating Bribery of Foreign Public Officials in International Business Transactions) is a convention of the OECD aimed at reducing corruption in developing countries by encouraging sanctions against bribery in international business transactions carried out by companies based in the Convention member countries. Its goal is to create a truly level playing field in today's international business environment.

Countries that have signed the convention are required to put in place legislation that criminalizes the act of bribing a foreign public official. The OECD has no authority to implement the convention, but instead monitors implementation by participating countries. Countries are responsible for implementing laws and regulations that conform to the convention and therefore provide for enforcement. The OECD performs its monitoring function in a two-phased examination process. Phase I consists of a review of legislation implementing the conventions in the member country with the goal of evaluating the adequacy of the laws. Phase 2 assesses the effectiveness with which the legislation is applied.

The Convention is open to accession by any country which is a member of the OECD or has become a full participant in the OECD Working Group on Bribery in International Business Transactions. As of May 2013, 40 countries have ratified or acceded to the convention:

Presently India is not a member of the OECD Anti-Bribery Convention.

V. U.N. Convention against Corruption

The United Nations Convention against Corruption (UNCAC) is a multilateral convention negotiated by members of the United Nations. It is the first global legally binding international anti-corruption instrument. In its 71 Articles divided into 8 Chapters, UNCAC requires that States Parties implement several anti-corruption measures which may affect their laws, institutions and practices. These measures aim at preventing corruption, criminalizing certain conducts, strengthening international law enforcement and judicial cooperation, providing effective legal mechanisms for asset recovery, technical assistance and information exchange, and mechanisms for implementation of the Convention, including the Conference of the States Parties to the United Nations Convention against Corruption (CoSP).

Chapter 15

Framework on Fraud Deterrence and Post Event Punishment

In the current world where frauds and the financial and the other ancillary losses due to frauds are on rise India as a country needs to have a pragmatic and strict approach towards fraud prevention, detection and timely and punishment to the fraudster which is commensurate with the nature and the scale of his offence. Fraud Deterrence is the key here as a significant amount of work gets done if the fear of consequence hovers around the head of person perpetrating a fraud .If a person fears the consequences of the act he shall have very serious thought before going ahead with the act and until now India as a country has taken very few steps in this regard. Unlike other countries like United States, Canada and United Kingdom to name a few, India does not have a separate legislation which deals with punishment of the fraudster.

Banking Sector

Perpetrators of frauds in banking transactions are liable to be prosecuted under the criminal law of the country for which adequate provisions of punishment have been prescribed under the Indian Penal Code, 1860.

Circular No. RBI/2014-15/85 by **RBI** dated 1st July 2015 on Fraud Classification and Reporting in Banking Sector – Gives classification of Frauds based on the provisions of the Indian penal code mainly to have uniformity in reporting.

As mandated Bank have to submit details of the Faraud in the return to RBI for cases which involve amounts of greater than Rs.1 lakh.

Insurance Sector

Circular No. IRDA/SDD/MISC/CIR/009/01/2013 dated 21st January 2013 on Insurance Fraud Monitoring Framework issued by **IRDA** mentions Fraud in Insurance Sector

The Guidelines mandate insurance companies to put in place, as part of their corporate governance structure, Fraud detection and mitigation measures; and to submit periodic reports to the Authority in the formats prescribed herein.

Securities and Exchange Board of India (SEBI)

Securities And Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices Relating to Securities Market) Regulations, 2003 deals with the frauds in case of Securities. The regulation recognizes the following cases as frauds

- Indulging in an act which creates false or misleading appearance of trading in the securities market;
- Dealing in a security not intended to effect transfer of beneficial ownership but intended to operate only as a device to inflate, depress or cause fluctuations in the price of such security for wrongful gain or avoidance of loss
- Advancing or agreeing to advance any money to any person thereby inducing any other person to offer to buy any security in any issue only with the intention of securing the minimum subscription to such issue
- Paying, offering or agreeing to pay or offer, directly or indirectly, to any person any money or money's worth for inducing such person for dealing in any security with the object of inflating, depressing, maintaining or causing fluctuation in the price of such security
- Any act or omission amounting to manipulation of the price of a security
- Publishing or causing to publish or reporting or causing to report by a person dealing in securities any information which is not true or which he does not believe to be true prior to or in the course of dealing in securities
- Entering into a transaction in securities without intention of performing it or without intention of change of ownership of such security
- Selling, dealing or pledging of stolen or counterfeit security whether in physical or dematerialized form
- An intermediary promising a certain price in respect of buying or selling of a security to a client and waiting till a discrepancy arises in the price of such security and retaining the difference in prices as profit for himself
- An intermediary providing his clients with such information relating to a security as cannot be verified by the clients before their dealing in such security
- An advertisement that is misleading or that contains information in a distorted manner and which may influence the decision of the investors
- An intermediary reporting trading transactions to his clients entered into on their behalf in an inflated manner in order to increase his commission and brokerage
- An intermediary not disclosing to his client transactions entered into on his behalf including taking an option position
- Circular transactions in respect of a security entered into between intermediaries in order to increase commission to provide a false appearance of trading in such security or to inflate, depress or cause fluctuations in the price of such security
- Encouraging the clients by an intermediary to deal in securities solely with the object of enhancing his brokerage or commission

- An intermediary predating or otherwise falsifying records such as contract notes
- An intermediary buying or selling securities in advance of a substantial client order or whereby a futures or option position is taken about an impending transaction in the same or related futures or options contract
- Planting false or misleading news which may induce sale or purchase of securities

The step which comes ahead of Fraud Deterrence or Prevention is Fraud Detection. In India there are several governmental as well as non-governmental organizations which are dealing with Fraud Detection.

- Serious Fraud Investigation Officer (SFIO)
- Central Bureau of Investigation (CBI)
- Enforcement Directorate (ED)
- Financial Intelligence Unit – India (FIU-IND)
- Private Organizations
- Fraud Containment Units

Serious Fraud Investigation Officer (SFIO)

The **Serious Fraud Investigation Office** (SFIO) is a multidisciplinary organization to investigate serious financial frauds. India. It is under the jurisdiction of the Government of India. The SFIO is involved in major fraud probes and is the coordinating agency with the Income Tax and CBI. The Serious Fraud Investigation Office is a multi-disciplinary organization having experts from financial sector, capital market, accountancy, forensic audit, taxation, law, information technology, company law, customs and investigation. These experts have been taken from various organizations like banks, Securities & Exchange Board of India, Comptroller and Auditor General and concerned organizations and departments of the Government. The Government approved setting up of this organization on 9 January 2003 on the basis of the recommendations made by the Naresh Chandra Committee which was set up by the government on 21 August 2002 on corporate governance.

Central Bureau of Investigation (CBI)

The **Central Bureau of Investigation** (**CBI**) is the foremost investigating police agency in India, an elite force which plays a role in public life and ensuring the health of the national economy. The CBI is responsible for investigation of cases which involve cases of bribery and corruption too notably 2G Scam, Coal Allocation Scam, Bofors Case etc. It is under the jurisdiction of the Government of India. The CBI is involved in major criminal probes, and is the Interpol agency in India. The CBI was established in 1941 as the Special Police Establishment, tasked with domestic security. It was renamed the Central Bureau of Investigation on 1 April 1963. Its motto is "Industry, Impartiality, Integrity".

Agency headquarters is in the Indian capital, New Delhi, with field offices located in major cities throughout India. It is headed by a Union Minister who reports directly to the Prime Minister. While analogous in structure to the Federal Bureau of Investigation in the United States of America, the CBI's powers and functions are limited to specific crimes by Acts.

Enforcement Directorate (ED)

The Directorate General of Economic Enforcement is a law enforcement agency and economic intelligence agency responsible for enforcing economic laws and fighting economic crime in India. It is part of the Department of Revenue, Ministry of Finance. The origin of this Directorate goes back to 1st May, 1956, when an 'Enforcement Unit' was formed, in Department of Economic Affairs, for handling Exchange Control Laws violations under Foreign Exchange Regulation Act, 1947.

The prime objective of the Enforcement Directorate is the enforcement of two key Acts namely, the Foreign Exchange Management Act 1999 and the Prevention of Money Laundering Act 2002

The main functions of the Directorate are as under

- Investigate contraventions of the provisions of Foreign Exchange Management Act, 1999(FEMA) which came into force with effect from 1.6.2000. Contraventions of FEMA are dealt with by way of adjudication by designated authorities of ED and penalties upto three times the sum involved can be imposed.
- Investigate offences of money laundering under the provisions of Prevention of Money Laundering Act, 2002(PMLA) which came into force with effect from 1.7.2005 and to take actions of attachment and confiscation of property if the same is determined to be proceeds of crime derived from a Scheduled Offence under PMLA, and to prosecute the persons involved in the offence of money laundering. There are 156 offences under 28 statutes which are Scheduled Offences under PMLA.
- Adjudicate Show Cause Notices issued under the repealed Foreign Exchange Regulation Act, 1973 (FERA) upto 31.5.2002 for the alleged contraventions of the Act which may result in imposition of penalties. Pursue prosecutions launched under FERA in the concerned courts.
- Sponsor cases of preventive detention under Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974(COFEPOSA) in regard to contraventions of FEMA.
- Render cooperation to foreign countries in matters relating to money laundering and restitution of assets under the provisions of PMLA and to seek cooperation in such matters.

Financial Intelligence Unit – India (FIU-IND)

- Financial Intelligence Unit – India (FIU-IND) was set by the Government of India vide O.M. dated 18th November 2004 as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

Private Organizations

Private Fraud Detection Organizations including CA Firms also play a vital role in investigating and detecting frauds for their respective clients. Such non-governmental organizations provide services flexible to the need of their clients. In additions several large organization have fraud prevention and deterrence departments which are include as part of the organizational structure. Some of these are headed by very senior personnel with exposure to both IT as well as the business. In organizations where data security and cyber threats are critical these positions may even report to the CEO to allow independent functioning

Chapter 16
Fraud Prevention

Fraud prevention is a topic applicable to many industries including banking and financial sectors, insurance, government agencies and law enforcement, and more. Fraud attempts have seen a drastic increase in recent years, making fraud prevention more important than ever. Despite efforts on the part of the institutions, hundreds of millions of rupees are lost to fraud every year.

An important early step in fraud prevention is to identify factors that can lead to fraud. What specific phenomena typically occur before, during, or after a fraudulent incident? What other characteristics are generally seen with fraud? When these phenomena and characteristics are pinpointed.

While Fraud may not be prevented altogether the focus of all prevention systems is three fold

(i) Making it as difficult as possible for frauds to occur. Here the mandate would be that all reasonable controls commensurate with the size and nature of the business would be in place

(ii) Definition of an exception reporting system and a compensatory control mechanism which ensures triggers and alerts in the event unusual behavioural or transactional patterns are observed

(iii) Verifying that the exceptions are reviewed by Management and the actions taken reflect that the reports are being followed up until a satisfactory explanation is obtained or investigative processes initiated

Effective Internal Controls

There are several keys to effective fraud prevention, but some of the most important tools are strong internal controls. Equally important, though, are the entity's attitude towards fraud, internal controls and an ethical organizational culture.

According to the Committee of Sponsoring Organizations (COSO), Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

(i) Effectiveness and efficiency of operations,

(ii) Reliability of financial reporting

(iii) Compliance with applicable laws and regulations.

Internal controls should not be thought of as "static." They are a dynamic and fluid set of tools which evolve over time as the business, technology and fraud environment changes in response to competition, industry practices, legislation, regulation and current economic conditions.

While no entity, even with the strongest internal controls, is immune from fraud, strengthening internal control policies, processes and procedures definitely makes them a less attractive target to both internal and external criminals seeking to exploit internal control weaknesses.

Strengthening internal controls is seldom accomplished by enhancing one process; rather it involves a comprehensive review of the risks faced, the existing internal controls already in place and their adequacy in preventing fraud from occurring. An internal control review may be conducted corporate-wide or on a location by location basis, or broken down to the individual business unit level. Generally, a review of this nature involves an in depth examination of people, processes and technology. However, there are other intangibles that organizations can not afford to overlook.

Audit Interaction

The first part of strengthening internal controls involves changing the attitude some employees have towards auditors. While it is easy to view auditors as the police department's "Internal Affairs" group—whose sole responsibility it is to ferret out wrongdoing—identifying employees who are breaking the rules, personal and professional success is to be had by viewing auditors as key partners and allies in the battle against fraud. This is further reinforced as the auditor's role ensures that he or she is always at the forefront of corporate policies, practices, procedures, technology, new products and services, making auditors a valuable source of corporate information

Secondly, part of strengthening internal controls is simply a matter of defining, or clarifying, ownership roles and responsibilities.

A common misperception among corporate employees is that internal controls are solely the responsibility of the company's Audit Department. While internal auditors measure the effectiveness of internal control through their efforts, they don't generally assume ownership. They assess whether the controls are properly designed, implemented and working effectively and make recommendations on how to improve internal control.

According to the Institute of Internal Auditors (IIA), "responsibility for the system of internal control within a typical organization is a shared responsibility among all the executives, with leadership normally provided by the CFO."

Systems Security Audits

With the growing need for security measures and the limited number of technical staff to meet the demands for the ever-increasing threat of unauthorized intrusion into an organization’s networking system, security audits have become one of several lines of defense employed to

help mitigate such action. According to Haynes (2003), a security audit is a process that can verify that certain standards have been met and identify areas in need of remediation or improvement. Dark and Poftak (2004) add that a computer security audit involves a systematic, measurable technical assessment of how the organization's security policy is employed at a specific site or location.

Haynes (2003) further explains that a security audit is a policy-based assessment of the procedures and practices of a site, assessing the level of risk created by these actions. A security audit comprises a number of stages. You can choose to focus the audit on different areas, such as the firewall, host, or network. However, a security audit will address issues with your systems, including software and hardware, your infrastructure, your procedures, your business processes, and your people. Information is the key. Once the audit has been completed you will have information on the compliance level of the users and systems under your control, with an idea of the risk exposure and security level of these systems. In some cases management may choose to carry out an audit internally or use an external contractor. Whoever carries out the audit, those personnel should have the relevant technical expertise and ability to communicate the findings of the audit. Even authorized system users can be the source of a security breach, therefore identifying possible lapses that could allow this is just as important as preventing external attack. It is important to understand that information security or computer security audits must move beyond information technology audits, which are concerned with ideas of auditing what is on the computer system and how it is being used. Instead security audits must also move past the review of programs and hardware, to the level of verifying that programs are operation with full integrity as they are intended to operate. . Security audits also must encompass components that ensure the data and information are reliable, as well as to verify that the information has not been compromised.

Security audits can be part of an information technology audit conducted by a team of professionals with expertise not only in the theoretical underpinnings of information systems, but also in the computer or networking system being audited. In addition, security audits must go beyond the annual financial audits and physical inventory audits to the data and content, which are standard processes in most businesses.

Methods for Performing Security Audits

When performing a security audit, one must perform the audit though personal interviews, vulnerability scan examination of operating system settings, analyses of network shares, and historical data. Those who conduct the audit should be concerned primarily with how security policies, the foundation of any effective organizational security strategy, are actually applied and implemented. According to Haynes (2003), there are a number of key questions that security audits should attempt to answer concerning the audit:

- Are passwords difficult to crack?
- Are there access control lists (ACLs) in place on network devices to control who has access to shared data? Are there audit logs to record who accesses data?

- Are the audit logs reviewed?
- Are the security settings for operating systems in accordance with accepted industry security practices?
- Have all unnecessary applications and computer services been eliminated for each system?
- Are these operating systems and commercial applications patched to current levels?
- How is backup media stored? Who has access to it? Is it up to date?
- Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan?
- Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?
- Have custom-built applications been written with security in mind?
- How have these custom applications been tested for security flaws?
- How are configuration and code changes documented at every level? How are these records reviewed and who conducts the review?
- What is the mechanism for providing data for testing? Are masking techniques used for maintaining data privacy
- How frequent and effective are the log reviews for
    - Databases
    - Applications
    - Network
    - Server activities
    - Intrusion Detection Systems wherever deployed
- What controls and measures are in place for misuse of admin passwords? Does the sensitivity of operations required a Privileged Account Management System.

Chapter 17
Organizations to Combat Fraud in India and Abroad

List of institutional framework in India to combat fraud in India

(i) Serious Fraud Investigation Office (SFIO)

(ii) Public Accounts Committee - examines the appropriateness of the expenditure incurred by the government as presented in the accounts, the reported cases of losses, financial irregularities in the government, and so on.

(iii) Comptroller and Auditor-General - the constitutional authority charged with the responsibility of auditing all receipts and expenditure of the Union Government and that of the States and Union Territories and agencies under them.

(iv) Chief Secretary - the highest administrative authority dealing with complaints of misconduct and fraud committed by any Department of the State.

(v) Crime Investigation Department (CID) - white collar crime and larger issues like scams and frauds are dealt by the Crime Investigating Department.

(vi) Economic Offences Wing - investigates cases pertaining to misappropriation, cheating, forgery, counterfeit currency, cybercrimes and major frauds, scams and other white collar offences.

(vii) Central Vigilance Commission (CVC) - The Central Vigilance Commission supervises corruption cases in governmental departments. It has supervisory powers over the CBI but does not have authority to prosecute individuals.

(viii) State vigilance Commission

(ix) Lokayuktha & UpaLokayuktha

(x) Central Bureau of Investigation (CBI) – it is a Governmental organization which normally investigates and prosecutes cases of serious fraud or cheating that may have ramifications in more than one state. It also investigates corruption cases.

(xi) Central Economic Intelligence Bureau (CEIB) - The Central Economic Intelligence Bureau monitors economic offences and co-ordinates co-operation with international agencies in relation to economic offences

(xii) Directorate of Enforcement (DOE) - Enforcement of Foreign Exchange Management Act 1999 and the Prevention of Money Laundering Act 2002. The organization falls under the Ministry of Finance and is headquartered in New Delhi

(xiii) Economic Intelligence Council (EIC) - Established under the Ministry of Finance to facilitate co-ordination among the enforcement agencies dealing with economic offences.

List of institutional framework outside India

(i) Serious Fraud Office (United Kingdom) - http://www.sfo.gov.uk/

The Serious Fraud Office (SFO) is an independent UK Government department that investigates and prosecutes serious or complex fraud and corruption. Accountable to the Attorney General, it has jurisdiction over England, Wales and Northern Ireland and assists a number of overseas investigations by obtaining information from UK sources. Section 2 of the Criminal Justice Act, 1987 grants the SFO special compulsory powers to require any person (or business/bank) to provide any relevant documents (including confidential ones) and answer any relevant questions including ones about confidential matters.

The SFO is also the principal enforcer of the Bribery Act 2010, which has been designed to encourage good corporate governance and enhance the reputation of the City of London and the UK as a safe place to do business.

The SFO is a specialist organization that investigates only the most serious types of economic crime. As a result a potential case must meet certain criteria before it is taken on.

(ii) National Fraud Authority (NFA) - https://www.gov.uk/government/organisations/national-fraud-authority

The National Fraud Authority is an executive agency of the United Kingdom Home Office responsible for increasing protection for the UK economy from the harm caused by fraud. The NFA works with a wide range of partners with the aim of making fraud more difficult to commit in the UK. Formerly the National Strategic Fraud Authority, it was set up in October 2008 in response to the government's Fraud Review in 2006.

The NFA works to tackle frauds across the spectrum, but also works on fraud types and fraud issues that are a notable problem. The NFA also produces the Annual Fraud Indicator, which estimates the cost of fraud.

Action Fraud is the UK's national fraud reporting service, run by a private sector company called bss for the National Fraud Authority. Action Fraud is the place to go to get information and advice about fraud, as well as to report fraud. UK citizens can report fraud online (such as forwarding scam emails for inspection) or by telephone. When a fraud is reported to Action Fraud, victims are given a crime reference number and their case is passed on to the National Fraud Intelligence Bureau (NFIB), which is run by the City of London's police service. The Action Fraud website also has an A-Z of fraud describing different types of fraud, and offers prevention advice.

The National Fraud Authority publishes the Annual Fraud Indicator every year, which is the UK's comprehensive estimate of how much fraud costs the UK.

(iii) CIFAS - The UK's Fraud Prevention Service –http://www.cifas.org.uk/

CIFAS is a not-for-profit membership association representing the private and public sectors. CIFAS is dedicated to the prevention of fraud, including staff fraud, and the identification of financial and related crime. CIFAS operates two databases:

- National Fraud Database (NFD
- Staff Fraud Database (SFD)

CIFAS has 290 Member organizations spread across various business sectors. These include financial services, retail, telecommunications, customer service centres, call centres and public services. Although at present CIFAS Members are predominantly private sector organizations, public sector bodies may also share fraud data reciprocally through CIFAS to prevent fraud.

Members share information about confirmed frauds in the fight to prevent further fraud. CIFAS is unique and was the world's first not-for-profit fraud prevention data sharing organization. Since CIFAS was founded, CIFAS Members have prevented fraud losses to their organizations worth over £8 billion by sharing fraud data.

Chapter 18
Financial Statements Frauds

1. Introduction and Background

Fraud is a global phenomenon affecting all sectors of the economy. Fraud encompasses a wide-range of illicit practices and illegal acts, consisting of intentional deception or misrepresentation.

A fraud can be defined as “a deception or misrepresentation, knowingly or intentionally, made by an individual or entity, knowing that the misrepresentation could result into some unauthorized gains to the individual or to the entity or some other party”.

1.1. Mistakes are different from Frauds

It may be stated that there is difference between mistakes and frauds and the mistakes are not fraud. Mistakes are unintentional acts, which may not results into losses to others or gains to the maker of mistakes.

Following items or issues could be broadly termed as mistakes and not frauds:

a. An unintentional mistake in processing or gathering the information, based on which the financial statements are prepared,

b. An incorrect accounting estimates arising due to oversight or mis-representation of facts,

c. A mistake in application of accounting principles relating to recognition, classification, presentation or disclosure.

1.2. Characteristics of Fraud

1.2.1. Misstatements in the financial statements can arise either from a fraud or an error. The distinguishing factor between the fraud and error is “whether the underlying action that results into the misstatement of the financial statements, is intentional or unintentional”.

1.2.2. Although the term “fraud” is a broad legal concept, for the purposes of the Standard on Audit”, the auditor is concerned with fraud that results into a material misstatement in the financial statements. Two types of intentional misstatements are relevant to the auditor– (a) Mis-statements resulting from fraudulent financial reporting and (b) Mis-statements resulting from misappropriation of assets. Although the auditor may suspect or, in rare cases, identify the occurrence of fraud, the auditor does not make legal determinations of whether fraud has actually occurred.

2. Issue and Purpose

The main issue and purpose is to understand the nature of financial statements frauds (who does them - types of persons committing frauds), why do they do - purpose behind committing frauds, how they do - modus-operandi, etc.):

2.1. A Financial fraud can be broadly defined as a wilful or an intentional act, with the intention to deceive someone involving financial transactions, for certain personal gains. As such, a fraud could be essentially termed as a **crime**, and is also a violation of civil law. A number of fraud cases, involving complicated financial transactions, were committed by so called 'white collar criminals', such as, business professionals, who have specialized knowledge and a criminal intent.

2.1.1. Corporate financial frauds result into a deep rooted negative impact on the sentiments of investors and also the capital markets, in general. It is noted that the efforts being made in the direction of detection and also prevention of frauds at present, are considered to be grossly inadequate or rather insufficient for identification of all such occurrences in a timely manner.

2.1.1. Unscrupulous individuals (as they commit frauds intentionally for their personal gains) manipulate, or influence the activities of a business, with the intention of making money, or obtaining gains through illegal or certain unfair means. Fraud deceives the organization of its legitimate income and results into a loss of money, even goodwill and reputation. In frauds, the doers employ illegal and immoral, or unfair means.

It is essential that in order to protect the entities from becoming victims of frauds, entities take steps to develop certain processes, procedures and controls that prevents the employees from committing frauds and that effectively helps in detecting fraudulent activity, if it occurs. The fraud involving persons from the leadership level is known under the name “managerial fraud” and the one involving only entity’s employees is named “fraud by employees’ association”.

3. Who Commits Frauds?

3.1. Every day, there are news or reports about entities or corporations behaving in discreditable ways. Generally, there are three groups of business people, who commit financial statement frauds. They range from (a) Senior Management; (b) Middle and Lower-level Management and (c) Organizational criminals.

3.1.2. Senior Management commits accounting frauds so as to conceal true business performance and also to preserve their personal status and control and also to maintain personal income and wealth. Mid and lower-level employees tend to falsify financial statements related to their area of responsibility (for example, subsidiary, division or other unit with which they are associated) so as to conceal their poor performance and/or to earn performance-based bonuses.

Organizational criminals also falsify financial statements for obtaining loans, or they artificially inflate value of stock, which they plan to sell in a “pump-and-dump” scheme. While many

changes in financial audit processes have stemmed from financial statement frauds or manipulations, history and related research repeatedly demonstrates that a financial audit simply cannot be relied upon to detect fraud at any significant level.

3.1.3. Frauds like any other crimes, could be best explained by three factors:

(a) Supply of motivated offenders,

(b) Easy availability of suitable targets and

(c) Absence of capable guardians, control systems.

Therefore, a fraud typically includes three characteristics, which are known as “fraud triangle.”

4. What is a Financial Statement Fraud?

4.1. Financial statement frauds usually involve activities such as Manipulation of Financial Statements with an intent to defraud the readers thereof. By manipulation, the financial position of the Company or Corporation, appears to be sound, though the actual position is not so. In the process of manipulation, there is either overstatement of the assets, revenues and profits on one side or an understatement of liabilities, expenses and losses on the other side. However, the overall objective of the manipulation may sometimes even require the opposite action, e.g., concealing higher-than-expected revenues or profits in a good year, so as to help in the subsequent year, which is expected to be a tougher year.

4.1.2. As such, the financial statement frauds are deliberate and intentional misrepresentation of the financial condition of an enterprise, which is carried out through the intentional misstatement or omission of amounts or disclosures in the financial statements, so as to deceive the users of the financial statements and hide the true picture thereof.

4.1.3. When the books are cooked so as to suit the needs, what it means is that the fraudsters are trying to "buy more time" so as to fix the business problems that prevent their entities from achieving its expected earnings or complying with the loan covenants. Cooking of the books may also be done with an intent to obtain new or additional finances on renewal of the facilities that would otherwise not be granted or would be lower, if true and honest financial statements were provided to the lenders.

4.1.4. People intent on profiting from crime may commit financial statement fraudsso as to obtain loans, which they can later siphon off either for personal gains or to inflate the price of the company's shares, allowing them to sell their holdings or exercise stock options at a profit. However, in many past cases of financial statement frauds, the doers of frauds have hardly gained or even nothing personally in financial terms. Instead the focus appears to have been preserving their status as market leaders - a status that might have been lost had the real financial results been published promptly.

4.1.5. A financial fraud is commonly defined as "intentional misrepresentation that an individual or entity makes knowing that the misrepresentation could result into some unauthorised benefit to the individual or to the entity or some other party."

5. Causes or reasons for Financial Frauds or Why Financial Frauds do take place?

5.1.1 Greed for money and work pressure, are the most common factors compelling management to commit financial frauds and deceive investors and creditors.

5.1.2. Some examples of pressures on the managerial persons generally include following factors:

- For obtaining finance at favourable terms or in the case of existing finance, negotiating the same for still more favourable terms;
- Encouraging investment through Sale of Stock;
- Demonstrating increased earnings per share (EPS) or increased Year-on-Year (Y-on-Y) or Q-on-Q profits, thus allowing dividends or distribution pay-outs financial statement fraud;
- Dispelling negative market perceptions or sentiments;
- Obtaining a higher purchase price for acquisitions or sales;
- Demonstrating compliance with financing covenants;
- Meeting projections set for performance and investor expectations, receiving performance-related bonuses;
- • An overwhelming desire for personal gains;
- • High personal debts;
- • Feeling that their pay is not commensurate with responsibility;
- • Strong challenge to beat the system.

5.1.3. As stated earlier, the opportunity to commit and conceal the fraud often involves either complete absence of oversight or inadequate oversight by the Board of Directors or Audit Committee, weak or non-existent internal control measures, existence of unusual or complex transactions, accounting estimates that require significant subjective judgment by management, and ineffective internal audit staff. If there are reasons present that make it appear to be relatively easy to commit and conceal the fraud, the likelihood of occurrence of frauds are very high.

5.1.4. If top management is not committed to observing high standards of integrity and ethical values, the ability to rationalize dishonest behaviour will be greatly increased. Top management is responsible for establishing the environment within which all operations are conducted. Management's commitment to integrity and ethical values is perhaps the most important factor in minimizing the ability to rationalize dishonest behaviour. Ethical values and honesty must be stressed and top management must display these qualities.

The Management cannot just expect everyone else to display these qualities, until they themselves abide by these values and set examples for others to follow. A commitment to enforcing integrity and ethical values will greatly reduce the ability to rationalize the dishonest behaviour.

6. Financial Statement Frauds

6.1. Financial statement fraud can take many different forms, but there are several methods that are considered most common.

These include fictitious revenues, timing differences, concealed liabilities or expenses, improper disclosure, related-party transactions and improper asset valuations.

6.2. From the accounting perspective, typically revenues, profits or even assets are overstated, while on the other side, losses, expenses, or liabilities are understated. Overstating revenues, profits or assets makes a financially weak company to look stronger (as against its actual financial position), while understating losses, expenses and liabilities results into increased net worth and equity. Understating revenues or overstating expenses is also an indicative of management's efforts to reduce tax liability.

6.2.1. Another alternative to financial statement fraud involves cookie-jar accounting practices, wherein a firm would understate its revenues in one accounting period and maintain them as a reserve for future periods, when there are worse performances. Such a practice irons out or removes the appearance of volatility from the operations.

6.2.2. It is evident that improper revenue recognition, including fictitious revenues and timing differences, accounts for majority of all financial statement frauds. Fictitious revenues are entails recording transactions or figures, such as sales that are yet to take place. This involves creation of fictitious or manipulated transactions with the intent to enhance the reported earnings. It is also a form of fabrication.

6.2.3. Fabrication of revenue typically involves creating fake or phantom customers and sales. Artificial sales could also involve legitimate customers — by creating phony invoices or increasing quantities or prices.

In such a method, the fictitious transactions are reversed in the subsequent period or period. There are several ways in which such fabricated revenues can be detected. Knowledge of the business and the industry is critical to understand the organization's financial statements and what may have occurred.

6.3. Timing differences is another method of creating fictitious revenues. It involves recording of revenues and/or expenses in the improper or wrong period. Recognizing revenues early, much before it is earned, will immediately increase the organization's income using legitimate sales, rather than creating phony sales. Recording expenses in the unrelated or wrong period or periods is another way of increasing the income, which means that expenses are either postponed or they are recorded incorrectly.

Expenses are either typically capitalized or recorded in the subsequent period or periods, so the effects are not taken into the income statement. Depreciating or amortizing assets too slowly is another method of delaying recognition of expense. If the objective is to decrease income so as to minimize the tax liabilities, it might accelerate expenses in the current period. This could involve increasing the rate of depreciation or amortization on assets. It could also include treating expenses of capital nature as revenue expenditures.

6.4. Thus, a financial statement frauds could be termed as a deliberate or intentional mis-representation, misstatement or omission of some factual or material financial statement data, with sole motive to mislead the readers for the purpose of creating a false impression (better financial health than the actual position) of an organization's financial strength.

6.5. Often business houses resort to financial statements frauds with a motive to evoke investor's interest or for the purpose of obtaining bank approvals for financing, or as a justification for bonuses or increased salaries or to meet expectations of shareholders.

Top Management is generally the centre point of such frauds in the financial statements, as fraudulent financial statements are prepared and finalised the Top Management level or at the whims and fancy of the Top Management.

7. Different types of Financial Statement Frauds

7.1. The following are examples of different types of Financial Statement Frauds:

(a) Fictitious revenues

(b) Fabricating revenue

(c) Inadequate provisions for sales and returns

(d) Sales with conditions

7.2. Revenue in order to be recognised as income or earnings must be "earned" and also must be either "realized" or be "realizable", before it could be recognized in the financial statements. Revenue is considered as having been "earned", only if the entity or corporate has substantially completed what it must have done, so as to be entitled to the benefits under the contract. Putting it in other words, the entity or corporate should have fulfilled substantially all its obligations to the customer. Revenue is considered "realizable" only when the related assets so received are readily convertible into cash or claims to cash.

7.2.1. Revenue is generally earned and realized or stands as realizable, when all of the following criteria have been met:

(i) There is an evidence that an arrangement exists between two parties. The requirement that persuasive evidence of an arrangement exists is intended to ensure that there is an understanding between two parties about the specific nature and terms of a transaction, which has been finalized. Determining the proper accounting treatment for a transaction depends on evidence of the final understanding between two parties, because a change in terms could lead to a different conclusion regarding the revenue recognition model to apply.

(ii) Delivery of goods has taken place or completed or where services are involved, such services have been rendered. Unless delivery of the goods has taken place or services have been rendered, as the case may be, the seller cannot be treated as having completed his obligations under the terms of the arrangement, and therefore, the revenue should not be recognized. Delivery is generally deemed to have occurred when the customer gets title and assumes the risks and rewards of the ownership of such goods or services.

(iii) The price of goods or services between the sellers to the buyer is fixed or ascertainable. Whether the price is fixed or determinable, could depend on several factors, including payment terms, discounts, and rebates, which could vary from contract to contract or arrangement to arrangement. In determining whether the price is fixed or ascertainable or determinable, entities are supposed to evaluate all elements of the arrangement so as to ensure that amounts recognized as revenue are not subject to refund or adjustment.

(iv) Another important factor is "collectability of the amount" under the agreement or contract and should be reasonably assured. If the collection of sale proceeds, service charges or fees in an arrangement is not reasonably assured, the general principle of being realized or realizable is not met, and revenue recognition is precluded until collection is reasonably assured.

7.2.2. Revenue from a service transaction is subject to the same revenue recognition requirements as applicable to a transaction under product sales. Regarding the delivery requirement, if the service has been performed, it is considered as having been "delivered." Non-refundable up-front fees are normally recognized over contract terms, not immediately. Inconsequential or perfunctory services can often be ignored.

7.2.3. In some cases, recognition of revenue is deferred until even the final lap of service has been performed, where execution of the final lap of acts is a critical event. In other situations, the scenario of "proportionate performance" is used. As such, it is absolutely important that the time of recognition of revenue is properly ascertained or determined. For example, in cases of sales of goods, when should the revenue be recognized; viz., on receipt of the customer order or on completion of production or on the date of shipment or on actual delivery of goods to the customer? The decision as to when and how revenue should be recognised has a significant impact on the determination of net income for the year (i.e., the "bottom line") and thus, it is a critical element in the preparation of the financial statements. Revenue earned is often considered as crucial to the users of financial statements in assessing the performance and future prospects.

7.3. The main objectives of revenue recognition are to:

(a) Removal of inconsistencies and weaknesses in the existing revenue recognition standards by providing clear principles for revenue recognition in a robust manner;

(b) Provide a uniform revenue recognition model, which will improve comparability over a range of industries, companies and geographical boundaries; and

(c) Simplify the preparation of financial statements by reducing the number of requirements to which preparers must refer.

7.3.1. The key principles on which the issue is based – revenue is recognized upon transfer to the customer, measured at transaction price – are consistent with much of current practice.

Under the asset-and-liability approach, revenue is recognized by direct reference to changes in assets and liabilities that arise from an entity's contract with a customer, rather than by direct reference to critical events or activities as in the earnings process approach. The idea is that where an entity has a legally enforceable, non-cancellable contract, it should begin to recognize the assets and liabilities inherent in that contract.

While this approach does not change the final profit or loss on the completed contract, it opens up the issue of the timing of recognition, moving from the end of the transaction, where recognition has traditionally taken place, to the moment when an executory contract comes into existence, and then re-measuring as the transaction moves or progresses towards completion.

7.3.2. The key concepts underlying the proposed standard include the following:

(a) A contract-based revenue recognition principle will be employed. The underlying principle is that revenue recognition should be based on accounting for a contract with a customer. A contract with a customer is viewed as a series of enforceable rights and performance obligations - obtained rights to payment from the customer and assumed obligations to provide goods and services to the customer under that contract.

(b) Revenue will be recognized when and as performance obligations in the contract are satisfied. Revenue arises from increases in an entity's net position (a combination of rights and obligations) in the contract with a customer as a result of the entity satisfying its performance obligation under the contract.

(c) The entity satisfies a performance obligation when goods or services are transferred to a customer. Revenue is recognized for each performance obligation when an entity has transferred promised goods or services to the customer. It is assumed that the entity has transferred that good or service when the customer obtains control of it.

(d) Revenue recognized is the amount of the payment received from the customer in exchange for transferring an asset to the customer. Consequently, the transfer of goods or services is considered to be the transfer of an asset.

(e) The amount of revenue will be measured based on an allocation of the customer's consideration. An entity transferring goods or services at different times needs to allocate total consideration received to each performance obligation. At inception, the transaction price is allocated between the performance obligations on the basis of the relative stand-alone selling prices of the associated goods or services.

(f) Re-measurement of performance obligations should take place when they are deemed "onerous." The carrying amount of an onerous performance obligation is increased based on the entity's expected costs of satisfying that performance obligation, and a corresponding contract loss is recognized.

7.3.3. There are five steps in applying the core principle of the proposed standard:

(a) Identify the contract(s) with the customer: An entity should combine contracts with the same customer and account for them together, if they are entered into at or near the same time, and one or more of the following criteria are met:

(i) The contracts are negotiated as a package with a single commercial objective.

(ii) There is price interdependence between the contracts - i.e., the consideration in one contract depends on the other contract; or

(iii) The goods or services in the contracts are interrelated in terms of design, technology or function.

(b) Identify the separate performance obligations within the contract: As defined, a performance obligation is a promise in a contract with a customer to transfer goods or services to the customer. Performance obligations include promises that are implied by an entity's business practices, published policies, or specific statements if those promises create a valid expectation that the entity will fulfil. When an entity promises to provide a bundle of goods or services, the entity should account for it as a single performance obligation, if the goods or services are highly interrelated and the contract includes significant integration of those goods or services into an item, for which the customer has contracted.

An example is when an entity provides materials and services in constructing a building. Otherwise, the entity should account for a promised goods or services as a separate performance obligation, if both of conditions below are met:

(i) The good or service is distinct, and

(ii) The pattern of transfer of the good or service is different from that of other promised goods or services in the contract.

A good or service is distinct if either:

(i) The entity regularly sells the good or service separately, or

(ii) The customer can use the good or service either on its own or together with resources that are readily available to the customer. Readily available resources include goods or services that are sold separately by the entity or another entity, or resources that the customer has obtained from previous transactions or events.

(c) Determine the transaction price: As defined, the transaction price is the amount of consideration an entity receives, or expects to receive, in exchange for transferring goods or services to a customer, excluding amounts collected on behalf of third parties, such as taxes. This definition reflects uncertainty and implicit financing.

When determining the transaction price, the objective is to estimate the total amount of consideration to which the entity will be entitled under the contract. The estimate of the total consideration can be based on a probability-weighted amount or the most likely amount, depending on which method is most predictive of the amount to which the entity is entitled.

An entity should recognize the revenue allocated to a satisfied performance obligation if the entity is reasonably assured that it will be entitled to that amount. The issue of collectability is closely related to the measurement of the transaction price.

Customer's credit risk should be accounted for separately and should not impact the measurement of the transaction price. Therefore, an entity should recognize revenue based on the stated contract price allocated to a satisfied performance obligation. The entity should also recognize an allowance for the expected impairment loss from contracts with customer, to be shown as a contra revenue line item in the income statement. An entity should adjust the contract amount to reflect the time value of money if the contract includes a financing component that is significant to that contract. To determine if a contract has a significant financing component, an entity should consider various factors, including:

(i) The amount of cash to be paid at the time of transfer of the goods or service;

(ii) The timing difference between the transfer of goods or services and customer payment; and

(iii) The interest rate within the contract, whether explicit or implicit. If the period between customer payment and the transfer of goods or services to the customer is less than a year, an entity does not need to assess if a contract has a significant financing component.

(d) Allocate the transaction price to the separate performance obligations: An entity should allocate to each separate performance obligation the consideration it expects to receive in exchange for satisfying that performance obligation on a relative standalone selling price basis. If the standalone selling price of a good or service is highly variable, the entity should estimate a standalone selling price using a residual technique, i.e., taking the total transaction price and deducting the standalone selling prices of other goods or services in the contract.

Conversely, an entity should allocate a portion of the transaction price entirely to one performance obligation, if both of the following conditions are met:

(i) The contingent payment terms of the contract relate specifically to the entity's efforts to satisfy that performance obligation or a specific outcome from satisfying that separate performance obligation; and

(ii) The amount allocated to that particular performance obligation is reasonable, relative to all of the performance obligations and payment terms, including other potential contingent payments in the contract.

(e) Recognize revenue when a performance obligation is satisfied: An entity should recognize revenue when it satisfies a performance obligation by transferring the promised good or service to the customer. This is when the customer obtains control of the promised good or service, which is defined as being when it has the ability to direct the use of, and receive the benefits from, the good or the service.

This is based on the premise that the continuous transfer of control is different between goods and services. For goods, the performance obligation is satisfied at a point in time.

The indicators that the customer has obtained control of a good include:

(i) The customer has an unconditional obligation to pay;

(ii) The customer has legal title;

(iii) The customer has physical possession; and

(iv) The customer has the risks and rewards of ownership of the good.

For services, an entity is considered to have satisfied a performance obligation over time, if at least one of the following two criteria is met:

(i) The entity's performance creates or enhances an asset that the customer controls, as the asset is created or enhanced; or

(ii) The entity's performance does not create an asset with alternative use to the entity and at least one of the following is met:

  (a) The customer receives a benefit as the entity performs each task;

  (b) Another entity would not need to re-perform the task(s) performed to date if that other entity were to fulfil the remaining obligation to the customer without the benefit of any inventory controlled by the entity; or

  (c) The entity has a right to payment for its performance to date. If an entity promises to transfer both goods and services, the entity should first determine whether the goods and services are separate performance obligations. If they are separate, the entity should account for them as such. Otherwise, the entity should account for the bundle of goods and services as a service.

7.4. Contract acquisition costs should be capitalized to the extent that they are recoverable. Contract acquisition costs are such costs that the entity would not have incurred if the contract had not been obtained. The capitalized contract acquisition costs are to be presented separately on the statement of financial position and subsequently amortized on a systematic basis consistent with the pattern of transfer of the goods or services to which the asset relates. Concerning testing for onerous contracts, an entity will be required to recognize a liability and an expense if the remaining performance obligations in a contract are deemed to be onerous. The remaining performance obligations in a contract are onerous if the costs that relate directly to satisfying those remaining obligations exceed the amount of the transaction

price allocated to those performance obligations. This situation must be reassessed at each financial reporting date. This standard will add to the already-extensive set of required disclosures to be made in the financial statements. In order to assist the users of financial statements to understand the amount, timing and uncertainty of revenue and cash flows, the enhanced disclosures under the revised standard include information about contracts with customers and information about various judgments and changes in those judgments effected during the reporting period. Regarding the former category, this will include, as may prove useful, a disaggregation of revenue; maturity analysis of specific remaining performance obligations; and reconciliation from opening to closing total contract balances. Concerning the latter group, this will include information about judgments and changes in judgment about the timing of revenue recognition and determining and allocating the transaction price.

7.4.1. Companies can use numerous methods to engage in premature or fictitious revenue recognition. Following are the most common techniques:

Agreements or policies which grant liberal return, refund or exchange rights;

Side agreements;

Channel stuffing;

Early delivery of product

Contracts with multiple deliverables;

Soft sales;

Partial shipments; and

Up-front fees;

Bill and hold transactions;

Recording false sales to existing customers and false sales to fictitious customers;

Round tripping

Other forms of improper recognition:

Recognizing revenue on disputed claims against customers;

Holding the books open past the end of a period;

Recognizing income on consignment sales or on products shipped for trial or evaluation purposes; and

Improper accounting for construction contracts ; and

Sham related party transactions.

7.5. The following paragraph seeks to address the major classes of fraud, as well as innocent errors involving revenue recognition.

Revenue Timing:

7.5.1. Recording a revenue intentionally in the wrong accounting period, is a management technique, whereby the management manipulates the timing of the revenue for possibly a number of reasons. These reasons could include meeting performance levels and also to achieve target bonus levels for the top management, as well as boosting stock values for holders of shares and possibilities of options on shares.

7.5.2. Although the revenue is real, by recognizing it in the wrong accounting period or in a different time cycle, i.e., in the earlier period it can be used to project a healthier growth than the real trend, projecting future continued success, which in fact can often be maintained only by continued, ever-growing fraudulent acceleration of revenue.

By "borrowing forward" from future revenues creates what is ultimately an unsustainable aura of growth. When this is no longer possible to continue such a practice, the fraud gets exposed, usually with disastrous consequences for the stock price and for the management. Holding the books open for a few extra days at year-end, until enough sales have actually occurred to meet whatever target was being aimed for, has a long history.

7.5.3. There can be no justification for this action. This is a financial reporting fraud. One variation on this scheme involves a so-called "bill and hold" arrangement, whereby customers are encouraged to place larger-than-needed orders, usually near the end of a reporting period. The sales are recorded, but the goods are held by the reporting entity for release to the customer in later periods. The customer is not obligated to make immediate payment for the goods, so in effect this becomes similar to a consignment arrangement, which is not recognizable as a sale as per generally accepted accounting principles.

7.5.4. Sometimes the goods are actually delivered, but with side agreements permitting abnormal levels of returns for unsold goods. In other cases, delivery is made, not to the ostensible customer, but instead to a warehouse or other facility controlled by the seller, which typically is done to deceive auditors examining shipping documents to find support for purported revenue transactions.

Yet another situation or variation arises when though the revenue is recorded but the significant uncertainties still remain. Going by the accepted accounting principles, the revenue should not be recognised until the uncertainties are resolved completely, although this deception may not always be apparent, particularly to the auditors, who only sample test transactions and may not fully appreciate the conditions stipulated in each sales transaction. However, cash collections from such sales will, upon closer inspection, seemingly lag behind the normal pattern, because the customer will pay only when all agreed-to conditions have been met.

7.5.5. For a seller of goods, premature revenue recognition also requires that cost of goods sold be manipulated, so that a normal or expected relationship between sales and costs can be maintained during the pendency of the fraud. In many instances where premature or fictitious revenue methods have been employed, this aspect has been overlooked.

In these cases the fraud becomes more obvious, particularly when auditors examine disaggregated information, such as quarterly or monthly accounting data, where end-of-period anomalies will tend to be more visible.

7.5.6. In the case of service transactions, the same general principle holds, but may be more difficult to detect, as margins may vary to a somewhat greater extent from one transaction to the next, compared with multiple transactions in uniform goods. Recording revenue when services are still due is a fraud intended towards jacking up the revenues, but may be difficult to detect, and this will persist as a problem. Unless services have been rendered completely, the accounting principles prohibit booking the revenue.

However, it is too common for companies to (1) ignore percentage-of-completion contracts by taking the cash payments into income, (2) fail to record offsetting accruals for services paid for in advance, and (3) record refundable deposits as income.

7.6. Fictitious recognition of revenue

An even more fundamental form of revenue fraud involves booking entirely fictitious revenue. The objective is similar - namely, (a) to exaggerate current period revenues and profits, or (b) to distort growth or profitability patterns, thereby impacting stock valuation, executive bonuses, and so forth.

7.6.1. In this situation, bogus (not just premature) receivables are recorded and as such receivables are never collectable, such receivables are bogus. Concealing fictitious revenue will later on necessitate reversal or elimination of such fabricated receivables.

Such receivables will inevitably draw audit attention and auditors would seek for recognition of such receivables as bad debts, thereby bringing reduction in earnings, even if the auditors do not detect the actual fraud.

7.6.2. Achieving a successful fictitious revenue fraud will often involve “refreshing” the old receivables by transferring the balances to other, equally fictitious customers. In this way the age of the bogus customer obligations can be maintained within a historically normal range for such receivables. Transferring bad receivables balances to substitute customers will require non-cash entries, usually made in the general journal, where they should draw auditors’ attention. An alternative is to engage in “lapping” the receivables, or crediting collections on real receivables against the bogus ones. This leads to a never-ending pattern of applying later collections to cover prior misapplications of collections to the fraudulent receivables. Here, too, the need to continue this practice over an extended period increases the likelihood of eventual discovery, again with probable disastrous consequences.

7.7. Accounting Polices and Customer Contracts

Inquiries into alleged improper revenue recognition usually begin with a review of the entity’s revenue recognition policies and customer contracts. The auditor considers the reasonableness of the company’s normal recognition practice and whether the company has

done everything necessary to comply with. For example, if the company customarily obtains a written sale agreement, the absence of a written agreement becomes a “red flag”.

The review should begin with a detailed reading of the contract terms and provisions. Particular attention should be focused upon terms governing

(i) payment and shipment,

(ii) delivery and acceptance,

(iii) risk of loss,

(iv) terms requiring future performance on the part of the seller before payment,

(v) payment of up-front fees, and

(vi) other contingencies. The auditor must consider timing – particularly as it relates to the company’s quarter and year-end periods. In which periods were the sales agreements obtained? When was the product or equipment delivered to the buyer’s site? When did the buyer become obligated to pay? What additional service was required of the seller?

In the absence of a written agreement, the auditor should consider other evidences of the transaction, e.g. purchase orders, shipping documents, payment records, etc.

7.8. Improperly deferring earned revenue

7.8.1. If a company’s earned revenue significantly exceeds estimates for a reporting period, the company may improperly defer recording some of the earned revenue until a future unfavourable reporting period. This is a variation on the common “cookie jar reserves” fraud, whereby unwarranted expenses are accrued currently, depressing current period profits, only to be reversed in later, less profitable periods. Although deferring revenue is less commonly observed than is accelerated recognition, and may be improperly defended using the often-misunderstood accounting concept of conservatism, it is nonetheless still financial reporting fraud. Detection is somewhat more difficult, but can often be identified using the same approaches as are useful in uncovering premature revenue recognition frauds – namely, by examining disaggregated data and closely studying key financial ratios. There is little reason to expect that the incidences of such frauds will be altered when the new revenue recognition standards becomes effective, given the underlying motivations to smooth earnings and meet announced targets.

7.8.2. In summation, the history of financial reporting frauds has been filled with a wide range of creative devices to either accelerate revenue recognition or to outright fabricate revenues. Thus, preparers, auditors and users of financial statements should be prepared to devote time and attention to this markedly new mode of accounting.

8. Revenue Recognition Vs. Fraud

8.1. Improper recognition of revenue - either prematurely or of fictitious revenue – is the most

common form of displaying wrongful earnings (either inflated or otherwise). Premature recognition of revenue involves the recording of revenue generated through legitimate means, at any time prior to the time when it would be legitimately allowed. Premature recognition should be distinguished and understood separately from recognition of fictitious revenue derived from false sales (which have not taken place, but have been reflected in the accounting books as such) or to false customers (who do not exist at all and would later on necessitate reversal thereof).

8.1.2. According to AS 18, revenue from the sale of goods shall be recognised when all the following conditions have been satisfied:

(a) the entity has transferred to the buyer the significant risks and rewards of ownership of the goods;

(b) the entity retains neither continuing managerial involvement to the degree usually associated with ownership nor effective control over the goods sold;

(c) the amount of revenue can be measured reliably;

(d) it is probable that the economic benefits associated with the transaction will flow to the entity; and

(e) the costs incurred or to be incurred in respect of the transaction can be measured reliably.

As such, the revenue is to be recognized only after the earnings process is completed and the rights of ownership have passed from seller to buyer. Examples of rights of ownership include: possession of an unrestricted right to use the property, title, assumption of liabilities and transferability of ownership, insurance coverage and risk of loss. How revenue is actually defined is a highly complex issue, but fraud is not so complicated. It involves purposeful attempts to deceive, not good-faith disagreements on accounting treatments. The auditor will normally find that revenue recognition frauds can be sub-divided into three categories viz., (i) holding the books open past the end of the accounting period, (ii) recording revenue when services are still due and (iii) shipping merchandise before the sale is final.

8.2. Playing with time

Probably the most common method to illegally recognize revenue early is to hold the books open even after the end of the accounting period in order to accumulate more sales. Proper accounting cut-off tests prevent most of these problems, but not all.

8.3. Recording revenue when services are still due or yet to be completed

Unless services have been rendered completely, the accounting principles prohibit booking the entire revenue amount. But it is all too common for companies to (1) ignore percentage-of-completion contracts by taking the cash payments into income, (2) fail to record offsetting accruals for services paid for in advance, and (3) record refundable deposits as income.

8.4. Shipping merchandise even before the Sale is final

Often merchandise sent on consignment basis is counted as having been sold. In more than a few cases, companies—around the time of an audit—have shipped merchandise to private warehouses for storage and counted those shipments as sales.

9. Timing differences

Early revenue recognition

Recording expenses in the wrong period

9.1. Frauds due to timing differences

When management is required to show year on year improved performance, they generally either tend to show inflated earnings or resort to reduced expenses or losses. Sometimes the Top Management even resorts to fraudulent timing differences in order to show unrealistic and phony profits.

There are five basic methods Companies generally employ to reflect bogus or unrealistic profits. One of them is fraud in timing differences, also called as a cut-off date fraud. It normally involves one of two basic techniques: recording revenues early and/or postponing recording of expenses and liabilities.

9.1.1. A Checklist for Detecting Timing Differences

This checklist will help determine the risk that an entity's financial statements are overstated due to timing differences. The more of "yes" answers, the higher the risk.

(a) Compared with previous periods, have sales increased materially? Have product lines changed?

(b) Is the company trying to raise capital or borrow money?

(c) Whether the earnings of key management personnel substantially depend on or determined by the company revenues or sales?

(d) Has the company delayed or denied access to original records?

(e) Do cut-off tests show that the books were held open beyond the end of the accounting period so as to accumulate more sales? Have some of the sales been reversed in subsequent periods?

(f) Have unusually large sales have taken place or been reflected within a few weeks of the end of the accounting period?

(g) Were sales to customers towards the end of the accounting period that were on unusual or extremely favourable conditions?

(h) In the last month of the accounting period, are there material unsupported revenue entries in the sales journal?

(i) When compared with previous periods, is there any significant reduction in the cost of sales?

Does the company have any history of employing aggressive or dubious accounting practices?

(J) Concealed liabilities and expenses

Instances of omission of liability and/or expenses,

Omission of liability on account of warranty or product liability

10. Understatement Liabilities and Expenses

10.1 Understating liabilities and expenses mirrors overstating income and assets - both serve to inflate artificially earnings and/or strengthening the company's financial condition.

Auditors can use various analytical indicators to search for such schemes, including:

An increasing current ratio (current assets/current liabilities) or quick ratio (cash + marketable securities + net receivables/current liabilities) from one period to the next;

Unexpected improvements in gross margins from one period to the next;

Change in inventory with no simultaneous increase in accounts payable or accrued expenses between periods; and

A comparison of the percent change in the accrued expense account with revenues reveals that revenue is increasing faster than accrued expense payable.

10.2. In addition to the above analytical procedures, an auditor should also inquire accounting personnel so as to if they have ever been asked to postpone expenses until a subsequent period. Finally, the auditor should also:

Review expense ledger and perform cut-off test to ensure that expenses are recorded in proper period and not postponed until a subsequent period;

Review prior years expenses and liabilities and look for unusual trends;

Perform current or quick ratio analysis which may indicate the concealment of liabilities;

Examine account detail looking for unusual debits to liabilities which would have the effect of reclassifying an expense to the balance sheet and also improving the current ratio (certain levels of current ratio may be required for debt covenant compliance);

Consider performing data mining procedures to identify significant payments for further review to determine whether the payment should have been capitalized;

Review internal controls to ensure expenses are recorded in proper accounting period and not postponed until a subsequent period; and

Review expenditures to determine whether they are more appropriately classified as expenses.

11. Overstatement or Assets or Understatement of Liabilities

Improper reporting of assets is another way for companies to overstate or inflate their earnings. A direct relationship exists between overstatement of assets and understatement of liabilities on the balance sheet and the inflated earnings.

In many cases, perpetrators are looking for a place on the balance sheet to place the debit. Overstating an asset or understating a liability usually occurs in this situation. Accounts, such as inter-company and foreign currency exchange gain/ loss should not be overlooked, as these are potential places to hide the debits.

11.1. Common asset overstatement fraud schemes include:

Creating fictitious assets;

Manipulating balances of legitimate assets with the intent to overstate value;

Understating liabilities or expenses, including failing to record (or deliberately under estimating) accrued expenses, environmental litigation liabilities and other business problems;

Misstating inter-company expenses; and

Manipulating foreign currency exchanges.

11.1.2. An auditor can often become alert to the possibility of fictitious or over-inflated assets by inquiring as to whether the entity intends to secure financing. If the answer is yes and if that financing is contingent on the value of particular assets, such as receivables or inventory, that should lead the auditor to ask more questions and perform additional procedures to verify the existence, and location and value of these assets. As with certain other schemes, the auditor can most often detect these schemes by observing the company's operations and inquiring as to unusual items.

11.1.3. Users of financial statements tend to look unfavourably at companies with significant amount of debts. When liabilities or expenses are concealed, the company's equity, assets, and/or net earnings are inflated. Understating liabilities involves not recording accounts payable or accrued liabilities, recording unearned revenues as earned, not accounting for warranty or service liabilities, not recording loans or keeping liabilities off the books and not recording contingent liabilities. Detecting concealed liabilities or expenses can be accomplished using several different methods.

11.1.4. Perform a search for unrecorded liabilities by completing a cut-off test that compares vendors' invoices, receiving documents, and cash disbursements to determine when the liability was actually incurred. Trace amounts to the accounts payable sub-ledger on the balance sheet date. Examine the open invoice file to see if all open invoices are recorded. Examine subsequent disbursements to determine whether disbursements were made for liabilities that were not recorded. Confirm liabilities with vendors. Examine the minutes of board meetings, contracts and loan or lease agreements to ascertain whether there are

liabilities or covenants that are not being properly disclosed. Identify related parties and check that liabilities have not been "pushed" over to them. Calculate the current ratio of the company. If it is unusually high, it may be indicative of hidden liabilities.

12. Improper disclosures

Liability omissions

Significant events

Management fraud

Related-party transactions

Changes in accounting policy

12.1. Improper and Inadequate Disclosures

12.1.1. Financial statement fraud is not just limited to numbers. A company can also misrepresent the financial condition of the company through misstatements and omissions of the facts and circumstances behind the numbers. Improper disclosures can take various forms notably, misrepresentations, intentional inaccuracies, or deliberate omissions in:

Descriptions of the company or its products, in news reports, interviews, annual reports, websites, etc.

Management discussions and other non-financial statement sections of annual reports, other reports; and

Footnotes to the financial statements.

12.1.2. In all these instances, management has perpetrated a fraud on the readers of the financial statements by not providing sufficient information required to make an informed decision regarding the financial position of the company.

Non-disclosure or inadequate disclosure of facts that have severe impact on the financials and operations of the organisation. In such cases, the management avoids disclosure of certain events, more particularly those events that have occurred after the date of balance sheet, but have significant impact on the financial position. These events have taken place after the date of balance sheet, but before the issuance of the financial statements and if reported in the financial statements, it would have adverse impact on the users' sentiments or perceptions.

For example, fire occurred in the factory premises and destroying substantial portion of assets like factory machineries and building, resulting into stoppage of production activities. Restoring of the factory would need substantial resources and time. Since the event is substantial and hence needs to be reported in the financial statements, but reporting could adversely affect the investors or market sentiments about the organisation.

As such, the management would try to hide such incidence and try that the auditors do not report the facts in the financial statements.

12.1.3. It was noted that the management had instructed the employees and other related staff members to:

- Omit the disclosure from the financial statements.
- Destroy any documentation related to the contamination. The auditors informed senior management about the line items that will require adjustment to the financial statements.

12.2. General Comments/Lessons Learned: The omission of disclosure of subsequent events occurring after the balance sheet date and issuance date of the financial statements could mislead the reader who is otherwise unaware of those events.

Accounting Standard (AS) 4 (equivalent to IAS 10) on "Contingencies and Events Occurring After the Balance Sheet Date" that an entity shall recognize in the financial statements the effects of all subsequent events that provide additional evidence about conditions that existed at the date of the balance sheet, including the estimates inherent in the process of preparing financial statements. The auditor will need to review the figures within the financial statements and the disclosures and other information contained within them in order to form an opinion on whether the financial statements, as a whole, give a true and fair view of the agency's financial position.

13. Improper asset valuations

Inventory

Accounts receivable

Fixed assets

Business combinations

Fictitious or Inflated Investments

13.1 Inventory Schemes

Fraudulent asset valuations comprised nearly half of the cases of financial fraud statements. Misstatements of inventory, in turn, comprised the majority of asset valuation frauds.

Generally, when inventory is sold, the amounts are transferred to cost of goods sold and included in the income statement. An overvaluation of ending inventory will understate cost of goods sold and in turn, overstate net income.

13.1.1. Inventory schemes can generally fall into three categories:

Artificially inflating the quantity of inventory on hand;

Inflating the value of inventory by

Postponing write-downs for obsolescence;

Manipulating unit of measurement to inflate value;

Under-reporting provisions for obsolete inventory, especially in industries where products are being updated or have a short shelf life; and

Changing between inventory reporting methods (average costing, last invoice price, LIFO, FIFO, etc.);

Fraudulent or improper inventory capitalization.

13.2. Following are indicators an auditor can look for to detect possible inventory manipulation:

A gross profit margin, which is higher than expected;

Inventory that increases faster than sales;

Inventory turnover that decreases from one period to the other;

Shipping costs that decrease as a percentage of inventory;

Inventory as a percentage of total assets that rise faster than expected;

Decreasing cost of sales as a percentage of sales;

Cost of goods sold per the books that do not agree with the company's tax return;

Falling shipping costs while total inventory or cost of sales have increased; and

Monthly trend analyses that indicate spikes in inventory balances near year-end.

Inflating Inventory Quantity (Fictitious Inventory)

The simplest way to overstate inventory is to add fictitious items to inventory. Companies can accomplish this by creating fake or fictitious:

Journal entries;

Shipping and receiving reports;

Purchase orders; and

Quantities on cycle counts or physical counts.

Some companies even go as far as maintaining empty boxes in a warehouse.

The most effective way to confirm the inventory balance is to carry out physical verification of the client’s inventory, particularly at such times when an inventory count is being performed. In fact, the auditors should physically observe, test and inquire as to the amount of inventory on hand so as to satisfy themselves with respect to the methods of inventory taking and the measure of reliance placed upon the client’s representations about the quantities and physical condition of inventories. When the auditor cannot be satisfied as to the inventories, he or she must physically count the inventory and test transactions in that account. Where inventory is

stored outside the company site, such as public warehouses, auditors should conduct additional procedures to confirm balance.

The auditor should look for the following operational factors may arouse suspicions of fictitious inventory:

Inventory that cannot be easily physically inspected;

Unsupported inventory, cost of sales or accounts payable journal entries;

Unusual or suspicious shipping and receiving reports;

Unusual or suspicious purchase orders;

Large test count differences;

Inventory that does not appear to have been used for some time or that is stored in unusual locations;

Large quantities of high cost items in summarized inventory;

Unclear or ineffective cut-off procedures or inclusions in inventory of merchandise already sold or for which purchases are not recorded;

Adjusting entries which have increased inventory over time;

Material reversals of entries to the inventory account after the close of the accounting period;

Inventory that is not subject to a physical count at year end;

Improper or “accidental” sales that are reversed and included in inventory but not counted in physical observation (for example a company “accidentally” delivers a specifics product to a customer, tells the customer it was a mistake and requests the customer to send the product back); and

Excessive inter-company and interplant movement of inventory with little or no related controls or documentation.

13.3. Even physical observation, however, is not fool-proof. Even when an auditor can observe inventory, a company can still perpetrate fraud by:

Following the auditor during the course of the count and adding fictitious inventory to the items not tested;

Obtaining advance notice of the timing and location of the inventory counts thereby permitting the company to conceal shortages at locations not visited;

Stacking empty containers at the warehouse, which are not checked during the count;

Entering additional quantities on count sheets, cards, scanners, etc. that do not exist or adding a digit in front of the actual count;

Falsifying shipping documents to show that inventory is in transit from one company location to another;

Falsifying documents to show that inventory is located at a public warehouse or other location not controlled by the company;

Including consigned items as part of the inventory count; and

Including items being held for customers as part of the inventory count.

13.4. To deter management from inflating inventory during physical counts, the auditor should consider:

Reviewing company policy for inventory counts (frequency and procedures);

Inquiring as to whether all inventory shrinkages have been reported;

Inquiring and observe inventory at third-party locations/off-site storage locations;

Observing a physical inventory unannounced; and

Conducting physical inventories for multi –locations all on the same date.

13.5. Inflating Inventory Value

13.5.1. In terms of applicable Accounting Standards (AS-2), inventories are to be reported at the lower of replacement cost or market value (i.e., net realisable value or current replacement cost). Companies tend to inflate inventory value for a variety of reasons other than to boost earnings. For instance, a common reason to inflate the value of inventory is to obtain higher finance from banks using the inventory as a security. Higher the value of the inventory, the more the money the company will be able to obtain in the form of financing.

13.5.2. Inflating inventory value achieves the same impact on earnings as manipulating the physical count. Management can accomplish this simply by creating false journal entries designed to increase the balance in the inventory account. Another common way to inflate inventory value is to delay the write-down of obsolete or slow moving inventory, since a write down would require a charge against earnings.

Auditors, thus, should be fully aware of the items comprising inventory and their life cycles, particularly as it relates to that industry. In addition, during the physical observation of the inventory, the auditor must look for and inquire about older items that appear to be obsolete. Few or no write-downs to market or no provisions for obsolescence in industries where there have been changes in product lines or technology or rapid declines in sales or markets warrant further investigation as to why the company has not accounted for such declines even when the inventory in question may be relatively new.

13.5.3. When a potential inventory valuation problem is detected or suspected, the auditor should consider:

Inquiring of accounting personnel as to the company's inventory pricing policy and how they identify net realizable value mark-downs;

Inquiring of management, accounting and finance personnel as to whether the company has shown historical patterns in the past of over valuation (i.e., prior year write down which became value impaired);

Inquiring of accounting personnel as to whether they have ever been requested to delay inventory write downs due to obsolescence etc.;

Touring the warehouse looking for items which appear to be old or obsolete and asking warehouse personnel if stock is slow moving, damaged or obsolete;

Inquiring of accounting personnel if they are aware of any items being sold below cost; and

Inquiring of industry experts whether the products are saleable and at what cost.

13.6. Fraudulent or Improper Inventory Capitalization

With respect to inventory fraud however, companies will sometimes seek to inflate inventory by capitalizing certain expenditures associated with inventory, such as selling expenses and general and administrative overhead. Amounts that are actually expenses but have been improperly reported as additions to the asset balance, thereby artificially increasing inventory value.

Auditors and investigators need to be cognizant of the company's capitalization policies, as well industry practice with respect to the expenses in question. Moreover, the auditor should consider whether past accounting policies have been aggressive with respect to capitalization, which would tend to indicate the need for further investigation. Finally, the auditor should look for changes to standardized cost amounts that increase the amounts capitalized to inventory.

13.7. Misappropriation of Inventory

Inventory fraud in its most basic definition is the misappropriation of inventory from a business. There are three basic ways that inventory is stolen:

Physical removal of the inventory from the company location either after it has been purchased and delivered and without manipulation of the books and records or after it has been purchased but before delivery to the client;

False write offs or other credits to inventory;

Recording false sales of inventory.

13.7.1. Anyone with access to inventory can engage in misappropriation - - the difference between the schemes lies in how the theft is concealed. A purchasing officer, for example, will usually not be able to adjust inventory records, so those types of frauds will not be available to him. A sales person has access to sales records and this will cover his theft differently than the purchasing officer.

13.8. Conversion of Inventory

The most basic form of inventory theft is the physical conversion of existing stock. Adequate physical security, which is beyond the scope of this chapter, is the obvious solution.

Conversion of inventory before it has reached the company is more sophisticated. This form of conversion occurs by the perpetrator who has authority to order inventory without supervision and authorization. Once the inventory is ordered, the perpetrator can direct the location to which it is delivered. Prevention of this scheme requires stringent controls regarding the ordering and approval functions. All orders should also require adequate documentation including shipping records to verify that the inventory was actually delivered to the company location.

13.9. False Write-offs and Other Debits to Inventory

Employees with the authority to write off inventory as damaged or scrap (or lack adequate supervision) often perpetrate false write-off schemes. The company will not detect that the inventory is missing once it is written off in the books and records.

Companies can institute controls to deter inventory manipulation. In addition to adequate physical security, controls include independent verification of records and separation of incompatible functions such as purchasing as writing off of inventory. Inventory counts should be performed by people independent to the inventory records department, or by independent third parties. The supervisor should verify all write offs and monitor disposal. All entries on the perpetual system should be referenced to a purchase, sale, or other record. Periodic checks should be performed on those records.

13.10. False Sales of Inventory

False sale frauds are very similar to recording a fictitious sale in the inventory records of the business. The false sale is never recorded as a sale in the sales records, which are usually kept independently from the inventory records. As there is no sale and no amount to collect or bank, the “sale” is never recorded and thus never missed. Alternatively, the false credit sale may be recorded (probably under a false name) but the amount never collected and eventually written off. A variation of the scheme is for the perpetrator to skim the proceeds of a valid sale to a real purchaser and not record the sale and the payment for the sale that is misappropriated.

Sales frauds, like other misappropriation frauds, occur due to a lack of controls or a breakdown of the controls in the sales process. Sales department employees should be monitored. All sales should require appropriate authorization in addition to sufficient documentation to support the sale. Furthermore, the individuals in the sales department should not be in charge of monitoring or writing off receivables and should have no influence over that department.

The auditor should perform observations of physical inventory and compare the inventory account for discrepancies between physical inventory and books. The auditor should determine whether inventory purchases are properly authorized, reconciled, and in possession of the company. Independent departments should authorize sales, write offs and, other debits. Inventory data should be entered completely, accurately, and only once. Finally, the auditor

should ensure that spot checks verifying the existence of inventory are performed on a regular basis by departments' independent of the purchasing and sales departments or by independent third parties

14. Investment Schemes

Fraudulent investment schemes provide another method for a company to overstate assets. Similar to schemes relating to inventory and receivables, management can create fictitious investments or deliberately over-value existing ones.

As discussed below, the auditor must first be familiar with all of the entity's investments and understand their classifications. This knowledge is necessary to spot the red flags of potential fraudulent accounting practices. The auditor must also be aware of the current market status of all investments and must confirm that the entity's books and records reflect all increase or decreases in such status. In addition, the auditor should question all classifications of securities to ensure that they are indeed classified in a manner that is consistent with the company's intentions and not just done to recognize gain or forgo recognizing loss. The auditor should be also wary of losses on securities held as available for sale that are accumulating in the other comprehensive income account. The company must eventually take a charge for these losses either through a sale or through a permanent write down. Evidence of accumulating losses may lead the auditor to conclude that management is intentionally delaying the recognition of such a loss.

14.1. Fictitious Investments

Fictitious investments are similar to the creation of other fictitious assets. Indicia include:

Missing supporting documentation;

Missing brokerage statements; and

Unusual investments (i.e., gold bullion) or ones held in remote locations or with obscure third parties.

14.2. Follow up procedures an auditor can conduct include:

Confirming the existence of the investment by physical inspection or by confirmation with the issuer or custodian;

Confirming unsettled transactions with the broker-dealer;

Reviewing the minutes of board of directors meetings and the company's Treasury policies to ensure that all investments were authorized by the Board and that company policy was followed in the trading of and investment in securities; and

Reviewing internal controls to ensure that the duties of purchasing, recording, and custody are adequately segregated.

14.3. Manipulating the Value of Investments

Companies can also manipulate their financial statements by inflating the value of investments by misclassifying them or failing to record unrealized declines in market value for those investments.

According to AS 13, investments are classified as long term investments and current investments. Current investments are in the nature of current assets, although the common practice may be to include them in investments.

Investments other than current investments are classified as long term investments, even though they may be readily marketable.

14.3.1. Carrying Amount of Investments: The carrying amount for current investments is the lower of cost and fair value. In respect of investments for which an active market exists, market value generally provides the best evidence of fair value. The valuation of current investments at lower of cost and fair value provides a prudent method of determining the carrying amount to be stated in the balance sheet.

14.3.2. Valuation of current investments on overall (or global) basis is not considered appropriate. Sometimes, the concern of an enterprise may be with the value of a category of related current investments and not with each individual investment, and accordingly the investments may be carried at the lower of cost and fair value computed category-wise (i.e. equity shares, preference shares, convertible debentures, etc.). However, the more prudent and appropriate method is to carry investments individually at the lower of cost and fair value.

14.3.3. For current investments, any reduction to fair value and any reversals of such reductions are included in the profit and loss statement.

Investments classified as trading includes such investments which are bought and held principally for sale in the near term. Investments not classified as trading or as held-to-maturity are classified as available-for-sale securities.

Trading and available for sale securities are reported at fair market value and must be periodically adjusted for unrealized gains and losses to bring them to fair market value. Unrealized gains or losses from trading securities are included in income for the period. Unrealized gains or losses from changes held as available for sale are reported as a component of other comprehensive income.

Equity securities (i.e., common or preferred stock) on the other hand, can be classified only as trading or available for sale. Unrealized gains or losses from changes in fair market value are reported in earnings for trading securities and as a component of other comprehensive income for securities held as available for sale.

14.3.4. Long-term investments are usually carried at cost. However, when there is a decline, other than temporary, in the value of a long term investment, the carrying amount is reduced to recognise the decline. Indicators of the value of an investment are obtained by reference to

its market value, the investee's assets and results and the expected cash flows from the investment. The type and extent of the investor's stake in the investee are also taken into account. Restrictions on distributions by the investee or on disposal by the investor may affect the value attributed to the investment. 18. Long-term investments are usually of individual importance to the investing enterprise. The carrying amount of long-term investments is therefore determined on an individual investment basis.

14.3.5. Where there is a decline, other than temporary, in the carrying amounts of long term investments, the resultant reduction in the carrying amount is charged to the profit and loss statement. The reduction in carrying amount is reversed when there is a rise in the value of the investment, or if the reasons for the reduction no longer exist.

14.3.6. The transfer of a security between different categories of investments is required to be accounted for at fair value. Securities transferred from the trading category will already have had any unrealized holding gain or loss reflected in earnings. For securities transferred into the trading category, the unrealized holding gain or loss as on the date of the transfer are to be recognized in earnings immediately. For securities transferred into the available-for-sale category from the held-to-maturity category, the unrealized holding gain or loss at the date of the transfer must be reported in other comprehensive income. Securities transferred from available for sale to held to maturity report unrealized holding gain or loss as at the date of the transfer as a separate component of other comprehensive income and amortized to interest income over the remaining life of the security.

14.4. Generally, with respect to investments, auditors should consider inquiring of:

Management as to company policies regarding the recording of unrealised gains or losses on trading and available for sale securities; and

Accounting personnel as to they have been asked to:

Record held to maturity securities at anything but amortized cost;

Not record all unrealised gains and losses in available for sale and trading securities have been recorded and if not the reason; and

Postpone a write down of a debt security.

14.5. Misclassification of Investments

Investments are classified as long term investments and current investments. Current investments are in the nature of current assets, although the common practice may be to include them in investments.

Investments other than current investments are classified as long term investments, even though they may be readily marketable.

Companies can manipulate financial statements by intentionally misclassifying securities or transferring securities to a class that would trigger the recognition of gain or conversely

postpone the recognition of a loss. For example, a company might misclassify a security as held to maturity in order to avoid recognizing a decline of value in the current period. Similarly, transferring a security from held to maturity to either trading or available for sale, would permit the recognition of gains that had not been previously recognized.

The Treasury function most commonly decides the classification at the time that the security is acquired. Auditors should review any changes in classification for possible abuse.

14.6. Recording Unrealized Declines in Fair Market Value

Deciding whether to write down a security due to a permanent decline in value is highly subjective and ordinarily left to the discretion of management. Accepting a write down results in a charge against net income. The auditor, thus, should consider whether management has inappropriately failed to or delayed a write down an impaired security to inflate income.

15. Accounts Receivable Schemes

15.1. Companies can manipulate accounts receivable with the same techniques that they can manipulate inventory; that is, by creating:

Fictitious receivables; and

Inflating the value of receivables.

15.2. Analytics that may assist in detecting overstated receivables include:

A decrease in the company's quick or current ratio;

Unexplained decrease in accounts receivable turnover

Unexplained increase in days sales outstanding; and

An increase of the ratio of credit sales to cash sales.

15.3. Creating Fictitious Receivables

Fictitious receivables are generally similar to those in our discussion of fictitious earnings:

Unexpected increases in sales and corresponding receivables by month at period end;

Large discounts, allowances, credits or returns after the close of the accounting period;

Large receivable balances from related parties or conversely from customers with unknown names or addresses or which have no apparent business relation to the business;

Outstanding receivable increasing faster than sales;

Organizations that pay commissions based on sales, rather than the collection of the receivable;

Increased receivable balances accompanied by stable or decreasing cost of sales and corresponding improvement in gross margins;

Lengthening of aging of receivables or granting of extended credit terms;

Excessive write offs of customer receivable balances after period end;

Re-ageing of receivables;

Excessive use of account called “miscellaneous/unidentified customer”

Large unapplied cash balance;

Increased trend of past due receivables; and

Lack of adequate controls in the sales and billing functions.

15.4. As part of the inquiry process, the auditor should:

Inquire of finance personnel and management as to whether the company is trying to obtain financing secured by its receivables;

Inquire of sales personnel as to whether they have been pressured to create fictitious or fraudulent sales invoices;

Inquire of accounting or sales personnel as to whether they have been pressured to:

Overstate the value of receivables;

Create fictitious journal entries or invoices for the sales of inventory or assets; and

15.5. Inquire whether customers have been pressured to accept large volume orders close to the end of period. Fictitious receivables schemes can also often involve related parties, as related parties are more likely to assist in collusion and providing of false information to the auditor. Auditors should inquire into the legitimacy of receivables if they appear to involve a related party.

15.6. Inflating value of Receivables

15.6.1. Inflating the value of legitimate receivables has the same impact as creating fictitious ones. Accounting Principles require accounts receivable to be reported at the net realizable value. Net realizable value is the gross value of the receivable less an estimated allowance for uncollectible accounts. It requires companies to estimate the uncollectible portion of a receivable to determine the net realizable value of receivables. The preferred method to determine uncollectible receivables is to periodically record the estimate of uncollectible receivables as a percentage of sales, outstanding receivables, or based on an aging of outstanding receivables.

15.6.2. Under the allowance method bad debt provisions are recorded as a debit to bad debt expense (an income statement account) and a credit to allowance for doubtful accounts (a balance sheet contra receivable account). When all or a portion of the receivable becomes uncollectible, the uncollectible amount is charged against the allowance account. When receivables are recorded at their true net realizable value, the recording of a bad debt

provision decreases accounts receivable, current assets, working capital and most importantly, net income.

Companies circumvent these rules by underestimating the uncollectible portion of a receivable. Underestimating the value of the provision (i.e., the amount deemed uncollectible) artificially inflates the value of the receivable and records it at an amount higher than net realizable value.

15.6.3. Overvaluing receivables also serve to understate the allowance account, such that the provision is insufficient to accommodate receivables that in fact become uncollectible.

A related scheme is not writing off (or delaying the write-off) of receivables that have in fact become uncollectible. These schemes are relatively easy to execute given the subjectivity involved in estimating bad debt provisions.

15.6.4. Potential auditing procedures include:

Spending adequate time to review and understand the provision;

Inquiring of management and accounting personnel as to the reasoning behind the amount of the provision; and

Determining the reasonableness of the provision in relation to the true facts surrounding the receivables.

15.6.5. Indications of the potential overvaluation of receivables include:

Minimum bad debt provisions or reserves that appear to be inadequate in relation to prior periods;

A history of extending payment terms to customers with limited ability to repay;

A history of inadequate reserves for uncollectible receivables;

Deteriorating economic conditions, e.g., declining sales;

Deteriorating accounts receivable days outstanding;

Untimely reconciliations and/or reconciliations that are “back of the envelope”;

History of inadequate reserves for uncollectible receivables;

Net receivables (i.e., net of the allowance for doubtful account) which are increasing faster than revenues;

Uncollectible accounts which have been on the books for extended periods of time but have not been written off; and

Recorded disputes with a customer that may potentially threaten ability to collect.

15.6.6. Follow up procedures include inquiring of:

Company changes to its credit policy and the reason for such changes;

Management as to the reason for any change in the reserve rates or policy for reserves in accounts receivable;

The sales force and Credit Department about whether they have been pressured or requested to grant credit to customers who are not credit worthy;

The Credit Department if they have been requested to extend payment terms for certain customers;

The Credit Department to determine whether certain sales people have instructed them to approve a customer and to avoid/circumvent the normal approval process; and

The nature and details surrounding any disputes with customers.

16. Software Development

Costs associated with developing new software are to be treated as expenses until the point of technological feasibility. Technological feasibility is established upon completion of a detail program design or, in its absence, completion of a working model. Once the technological feasibility is established, all software production costs must be capitalized and subsequently reported at the lower of unamortized cost or net realizable value.

Whether technological feasibility has been reached is a subjective decision and thus subject to abuse. By arbitrarily determining technological feasibility, management can manipulate income by increasing or decreasing the amount capitalized or expensed. Auditors should consult with the company's technical personnel (i.e., engineers, programmers) in reviewing management's assertions that technological feasibility has been achieved.

17. Research and Development ("R&D")

In accordance with AS 26, no intangible asset arising from research (or from the research phase of an internal project) should be recognised.

Expenditure on research (or on the research phase of an internal project) should be recognised as an expense when it is incurred.

17.1. This Standard takes the view that, in the research phase of a project, an enterprise cannot demonstrate that an intangible asset exists from which future economic benefits are probable. Therefore, this expenditure is recognised as an expense when it is incurred.

17.2. Examples of research activities are:

(a) activities aimed at obtaining new knowledge;

(b) the search for, evaluation and final selection of, applications of research findings or other knowledge;

(c) the search for alternatives for materials, devices, products, processes, systems or services; and

(d) the formulation, design, evaluation and final selection of possible alternatives for new or improved materials, devices, products, processes, systems or services.

17.3. Development Phase:

An intangible asset arising from development should be recognised if, and only if, an enterprise can demonstrate all of the following:

(a) the technical feasibility of completing the intangible asset so that it will be available for use or sale;

(b) its intention to complete the intangible asset and use or sell it;

(c) its ability to use or sell the intangible asset;

(d) how the intangible asset will generate probable future economic benefits. Among other things, the enterprise should demonstrate the existence of a market for the output of the intangible asset or the intangible asset itself or, if it is to be used internally, the usefulness of the intangible asset;

(e) the availability of adequate technical, financial and other resources to complete the development and to use or sell the intangible asset; and

(f) its ability to measure the expenditure attributable to the intangible asset during its development reliably.

17.4. In the development phase of a project, an enterprise can, in some instances, identify an intangible asset and demonstrate that future economic benefits from the asset are probable. This is because the development phase of a project is further advanced than the research phase.

17.5. Examples of development activities are:

(a) the design, construction and testing of pre-production or pre-use prototypes and models;

(b) the design of tools, jigs, moulds and dies involving new technology;

(c) the design, construction and operation of a pilot plant that is not of a scale economically feasible for commercial production; and

(d) the design, construction and testing of a chosen alternative for new or improved materials, devices, products, processes, systems or services.

The acquirers tend to classify a large part of the acquisition price as in process research and development ("R&D"), thereby allowing the entity to immediately expense the costs. This practice allows the entity to write off the R&D in a single chunk in the year of acquisition itself

and not burdening future earnings with amortized R&D charges. This type of practice also involves the creation of liabilities for future operating expenses.

18. Start-up Costs

Similar to R&D, all start-up costs to be expensed or charged as revenue expenses in the year of expense itself. However, many entities will label start up activities as other costs, thereby attempting to capitalize them.

19. Interest Costs

19.1. According to Ind AS 23, an entity shall capitalise borrowing costs that are directly attributable to the acquisition, construction or production of a qualifying asset as part of the cost of that asset.

As such, the entity shall recognise other borrowing costs as an expense in the period in which it incurs them.

19.2. Where borrowing costs are directly attributable to the acquisition, construction or production of a qualifying asset are included in the cost of that asset. Such borrowing costs are to be capitalised as part of the cost of the asset, when it is probable that they will result in future economic benefits to the entity and the costs can be measured reliably.

19.3. Capitalization of Interest Costs, requires the capitalization of interest costs incurred during the acquisition and construction of an asset. The interest cost capitalized are added to the cost of acquiring the asset and then amortized over the useful life of the asset. The total interest cost capitalized in a period may not exceed the interest cost incurred during that period.

Capitalization is no longer allowed when the cost of the asset exceeds its net realizable value. One potential scheme in this area is for the company to continue capitalizing interest after construction has been completed.

20. Improper Capitalization of Expenses

Capitalization of company expenditures is another fertile area for abuse. The most common way is to record expenditures as capital items rather than ordinary expenses. This technique allows the company to capitalize and amortize the expense over many periods rather than recognize it in its entirety in the current period.

The start of any audit with respect to questionable capitalization policies should be the company's accounting policy with respect to this area in addition to the policies of other entities in the industry. Is the company being overly aggressive with its policies as compared to other companies? Due consideration must also be given to management's reasons for selecting the policy. The auditor will also want to consider whether the costs in question are providing future benefit thereby warranting capitalization. Detecting capitalization policies can often be achieved by considering or reviewing the following items:

Is there a heavy capitalization of fixed assets?

Are capitalized costs that are increasing faster than revenue over lengthy periods?

Are repair and maintenance expenses (or other operating expense) dropping out of line with operations (indicating these are possibly being capitalized instead of expensed?

With respect to construction contracts, does interest expense properly increase when construction and capitalization of expenditures has ceased?

Have prior accounting policies have been aggressive with respect to capitalization?

21. Advertising Costs

Reporting on Advertising Costs, provides that all advertising expenses must be expensed as incurred unless there exists persuasive historic evidence that allow the entity to make a reliable estimate of future revenue to be obtained as a result of the advertising in which case the expenditures are allowed to be capitalized.

22. Recording Fictitious Fixed Assets

Similar to the concept of recording fictitious sales or receivables, entities will record fictitious assets to improve the balance sheet which, as previously discussed, inflates earnings as well.

22.1. Fictitious assets include:

Fixed assets on books and records which do not have an apparent relation to the business;

Lack of a subsidiary ledger to record additions and retirements;

Lack of adequate policies and procedures to determine whether property and equipment are received and properly recorded;

Lack of procedures to account for fixed assets that may have been moved from one facility to another;

Existence of a second-hand storage facility for fixed assets that may still have useful life but for some reason are not being used;

Lack of adequate written policies and procedures concerning the recording, retirement and disposition of fixed assets; and

Sub-ledgers that do not reconcile to the general ledger.

22.2. Follow up procedures to consider if any of these indicia are present include:

Tour of the client's facility to review fixed assets: select certain fixed assets from the fixed asset listing (especially new, significant additions), physically confirming that the fixed asset exists and physically inspecting the asset's serial number if applicable;

Determine that retired assets are no longer included in financial statements; and

Review internal controls to ensure that there are written policies covering retirement procedures which include serially [sequentially] numbered retirement work orders, reasons for retirement and all necessary approvals.

23. Depreciation & Amortization Schemes

An easy way to inflate the value of an asset is to extend its depreciable/amortizable life so that it is carried on the books for a longer period. Depreciation is another area in which management is given leeway to choose any method so long is that method allocates the costs in a "rational and systematic manner."

Detection of these schemes begins with a review of the company's depreciation policy. Most companies have written policies for depreciating assets. Lack of a written policy heightens the potential for abuse as it enables management potentially to record depreciation on an ad hoc basis with no particular rational. Similarly, recent changes to the entity's depreciation policy should be scrutinized for both their purpose and effect on the entity's assets.

23.1. Auditors who have suspicions should consider:

Reviewing the records of depreciable assets for unusually slow depreciation or lengthy amortization periods;

Comparing prior years depreciation charges with current year for reasonableness;

Identifying changes in policy which may affect the rate of depreciation that appears to boost earnings;

Inquire into historical depreciation policies to determine the extent of their aggressiveness; and

Reviewing a detailed list of fixed assets as well as the assigned lives of the assets and then randomly selecting certain fixed assets and recalculating the net book value at reporting date based upon the recorded life of the asset.

24. Establishing Off-Balance Sheet Entities

24.1.The Enron scandal highlighted the practice of fraud by using "off-balance sheet" vehicles to transfer and conceal debt.The fraud occurs when companies use them to, for example, conceal debts, thereby misleading investors about the risks and rewards of a transaction, particularly when inadequate or misleading disclosure are provided. Off-balance sheet transactions also have an income statement impact as well.

24.2. With an off-balance sheet transaction, a company's "investment" account on the income statement will reflect the relevant proportion of net profit or loss that results from operation of the underlying net assets. In other words, the effect of non-consolidation should leave income the same as if the off-balance sheet investment had been consolidated. However, the individual line items composing that net income or loss are not explicitly shown. A consolidation treatment conversely, would show individual revenue and expense line items.

24.3 Off-Balance Sheet Treatment V/s Consolidation

Off-balance sheet transactions are transactions wherein a company retains the benefits of assets in a corporate vehicle not consolidated for financial accounting purposes. These investments can typically appear in the asset section of the balance sheet as a single net line item, titled variously as an "investment in affiliate", "retained interest in securitization", etc.

Off-balance sheet transactions enable the company to avoid showing the individual asset of the off-balance sheet vehicle in the balance sheet, and more importantly, the associated debt used to acquire the off-balance sheet vehicle's assets. In other words, the company executing the transaction reports only its proportion of the net assets of the off balance sheet vehicle as an asset, rather than reporting the gross assets of the vehicle, including the vehicle's total debt and outside interests held by other parties. While this form of reporting technically would not change the net equity of the company executing the transaction, the consolidated balance sheet would show greater total assets and greater total debt. Thus, in executing an off-balance sheet transaction, the company looks more financially attractive. In addition, there is an impact upon balance-sheet dependent financial ratios; for instance, it is likely that debt to equity ratios will be higher, and therefore less favourable, under consolidation treatment as compared to non-consolidation.

Off-balance sheet treatment has historically been used for among other things:

Securitization transactions - financial assets such as receivables are sold to an off-balance sheet vehicle while the seller retains a subordinated interest in that entity;

Leasing transactions – long-lived assets are acquired by an off-balance sheet entity. The use of the assets is conveyed to a third party via an operating lease; and

Non-controlling investments: assets or businesses are held by an entity that does not convey control back to the investors. One simple example is a jointly controlled joint venture. The assets and debt of that venture remains off-balance sheet for at least one of the partner/investors involved.

25. Overstatement of Liability Reserves ("Cookie Jar Reserves")

25.1. While most fraud schemes are geared toward inflating the current financial position, companies sometimes overstate the amount of provisions to cover the expected costs of liabilities such as taxes, litigation, bad debts, job cuts and acquisitions. In doing so, management will establish inflated accruals in those years where the company is extremely profitable and doing well and can afford to incur larger expense amounts. These "cookie jar reserves" are then tucked away for management to reach into and reverse in future years where the company is unprofitable or marginally profitable when a boost to earnings would be beneficial.

25.2. Company managers estimate reserves. The outside auditor judges whether the reserves are reasonable. Generally, it is difficult for auditors to challenge company estimates because there are no clear accounting guidelines. This creates a ripe environment for abuse.

26. Materiality

26.1. No discussion of financial statement fraud is complete without a discussion on materiality. Companies (and sometimes auditors) dismiss improprieties, because they are not considered as “material” to the financial statements.

26.2. An information is material if its omission or misstatement could influence the economic decisions of users taken on the basis of the financial statements.

Materiality, therefore, relates to the significance of transactions, balances and errors contained in the financial statements. Materiality defines the threshold or cut-off point, after which financial information becomes relevant to the decision making needs of the users. Information contained in the financial statements must, therefore, be complete in all material respects in order for them to present a true and fair view of the affairs of the entity.

26.3. Materiality is relative to the size and particular circumstances of individual companies.

Example - Size

A default by a customer who owes only Rs. 1000/- to a company having net assets of worth Rs. 10 million, is immaterial to the financial statements of the company.

However, if the amount of default was, say, Rs. 2 million, the information would be material to the financial statements, omission of which could cause users to make incorrect business decisions.

Example - Nature

If a company intends to curtail its operations in a geographic segment, which has traditionally been a major source of revenue for the company in the past, then this information should be disclosed in the financial statements, as it is by its nature material to understanding the entity's scope of operations in the future.

Materiality is also linked closely to other accounting concepts and principles:

(a) Relevance: Material information influences the economic decisions of the users and is therefore relevant to their needs.

(b) Reliability: Omission or mis-statement of an important piece of information impairs users' ability to make correct decisions taken on the basis of financial statements thereby affecting the reliability of information.

(c) Completeness: Information contained in the financial statements must be complete in all material respects in order to present a true and fair view of the affairs of the company.

26.4. Over time, companies and their auditors have also developed certain “rules of thumb” to assist them in determining when a matter might be deemed material. One frequently used rule of thumb is that a misstatement or omission that is less than 5% of some factor (i.e., net income or net assets, etc.) is not material.

While there should not be any objection to the use of the 5% threshold as a preliminary assessment of materiality, but exclusive reliance on quantitative benchmarks, such as the 5% rule can only be the beginning of a materiality analysis and not a substitute for a full analysis of one Examples of qualitative factors to be considered include whether the misstatements:

Arise from imprecise estimates;

Mask changes in earnings trends;

Cause financial statements to meet analysts' expectations;

Would change a loss to income or vice versa;

Affect compliance with regulations or contracts;

Affect management compensation; or

Arise from illegal acts.

Thus, it is clear that numerical tests also will no longer satisfy a materiality analysis and that the auditor must question the facts and circumstances surrounding all suspicious transactions and cannot simply pass on them if they are deemed financially immaterial.

27. Misappropriation of Cash

Cash schemes are the most common form of misappropriation of assets. The major categories include: (i) skimming and larceny of cash and (ii) fraudulent disbursements. Fraudulent disbursements include: (i) billing schemes, (ii) payroll schemes, (iii) expense reimbursement schemes, (iv) check theft and tampering of checks and (v) register disbursement schemes.

27. 1 Skimming of Cash

Unrecorded or Understated Sales or Receivables- (Failure to record the full amount of sales or other items of income)

27.2. Many asset misappropriation schemes start at the entry point of the sale. An employee can embezzle monies by not recording the sale or full amount of the monies received. Deterrence of skimming activities requires adequate segregation of duties among the individuals recording the sales, receiving the monies, and recording the sales in the books. In addition, particular attention must be paid to those individuals, such as consultants and sales people, who handle cash in offsite locations. These individuals often operate without sufficient controls governing their conduct that can lead to the perpetration of this scheme.

27.3. Special attention should also be given to payments made on the account. Perpetrators can convert the cash and then either wait for an alternative source of funds to make up for the replace the funds converted (This practice, more commonly known as lapping, will be discussed in detail below). The perpetrator may simply not record the payment against the customer's account at all. The customer's receivable balance will remain unchanged or slightly changed despite the fact that they have been making payments. After the receivable has aged

significantly, the perpetrator writes off the receivable balance as unpaid. Adequate segregation of duties again is key. The same individual should not be in charge of recording and monitoring receivables in addition to being given the responsibility of authorizing and recording write offs.

27.4. The auditor should review the customer complaint log for complaints regarding the misapplication or lack of payment to their receivable account balance and follow-up on any recorded complaints with both management and the customer to see what the nature of the problem was, how it was resolved, by whom within the organization and finally whether the problem occurred subsequently.

27.5. The auditor should also consider performing certain analytics and noting particular trends such as:

Cash that is decreasing in relation to total current assets;

Cash that is decreasing in relation to credit sales;

Decrease in sales accompanied by an increase in cost of sales;

Current ratio which has decreased significantly from prior periods;

Decreasing gross margins from the prior to the current period;

Cash collections which are significantly less than reported revenues;

Significant amount of write offs in the current period as compared to the previous period; and

Decreasing trend of payments on accounts receivable.

27.6. Other indications of the existence of this scheme include:

Lack of segregation of duties between the sales, receipts and recording functions;

Poor controls over the completeness of recording sales;

Sharp increase in the average length of time that customer cash receipts are maintained in an account before being applied to customer's outstanding balance;

Periodic or large or numerous debits or other write offs to aged accounts;

Recorded customer complaints regarding misapplication of payments to their account;

Forced account balances such as overstatements of cash balances that are made to match the accounts receivable balance;

Numerous or significant reversing entries or other adjustments been made which have caused the books or register to reconcile to the amount if cash on hand; and

Large or numerous suspicious debit adjustments to aged receivable accounts.

27.7. Finally, an auditor confronted with these high risk factors should consider:

Inquiring of management or internal audit group whether there ever been previous problems with employee theft of incoming cash receipts;

Inquiring as to the company's policy for monitoring off site sales people (if applicable) or rental properties that generate cash flows for the company;

Inquiring on how reconciling items or discrepancies are treated and reviewed by management;

Inquiring of management and sales personnel regarding customer complaints about billing and/or payments not being applied to their accounts;

Following up with customers regarding any recorded complaints; and

Inquiring of management and others whether they are aware of any employees having financial difficulties.

28. Channel Stuffing

Channel stuffing refers to the practice of offering deep discounts, extended payment terms or other concessions to customers to induce the sale of products in the current period, when they would not have not been otherwise sold until later periods, if at all.

Channel stuffing often is indicated by an increase in shipments, which is usually accompanied by an increase in shipping sold at steep discount costs, at or near the end of period. Where these circumstances occur, the auditor or auditor should (i) inquire whether the goods were sold and (ii) review customer contracts and side agreements for unusual discounts in exchange for sales and rights of return provisions. The auditor should also inquire of sales personnel and shipping personnel regarding management influence to alter normal sales channel requirements.

In addition, customers offered deep discounts often purchase inventory in excess of required needs to take advantage of the reduced prices. This excess, inventory is often returned by the customer after the close of the period as it cannot be resold. The auditor thus should consider the amount of returns shortly after the close of a period as compared to prior periods and margins on sales recorded immediately before the end of a reporting period.

Early Delivery of Product

Shipping unfinished or incomplete products to customers, or at a time prior to when customers are ready to accept them;

Engaging in "soft sales" (shipping of products to customers who have not agreed to purchase);

Recognizing the full amount of revenue on contracts where services are still due to the client, and/or

Recognizing the full amount of revenue on fees collected up front.

Income should not be recognized under these circumstances because delivery has not actually occurred.

Customers on the other side of early delivery schemes often return the unfinished product or demand more completion before payment is rendered.

Analytics that may reveal the existence of an early delivery scheme include:

Comparing returns in the current period and prior periods;

Comparing shipping costs in current period and prior periods; and

Comparing shipping costs as a percentage of revenue in the current period and prior periods.

29. Lapping

Lapping generally involves converting one customer's payment and then using a subsequent payment, usually from another customer, to cover the payment converted from the previous customer's account. For example, the perpetrator steals the payment intended for customer A's account. When a payment is received from customer B, the thief credits it to A's account. And when customer C pays, that money is credited to B.

Lapping tends to increase at exponential rates and lapping schemes often tend to reveal themselves because the employee is unable to keep track or obtain additional payments to cover up the prior skimming.

The controls, analytical and other indicators that apply to skimming also apply to lapping. However, one of the most effective ways to control a potential lapping scheme is to require a daily bank deposit in addition to an independent confirmation that the deposit was properly made. Additionally, the auditor be aware, pay attention and inquire into any delays in the processing of payments to customer's accounts and inquire as to the reason for those delays.

30. Fraudulent Disbursements

Cash schemes involve the theft of revenues before they have been recorded in the books and records of the company. Fraudulent disbursement schemes, on the other hand, involve theft of funds already entered into the books and records. Fraudulent disbursement schemes generally fall into five main categories:

Billing schemes;

Theft of company checks;

Payroll schemes;

Expense reimbursement schemes; and

Register disbursement schemes.

These five categories in turn can be broken down further to include a host of other individual schemes many which, like the cash skimming schemes discussed above are similar in their nature and means of detection.

30.1. Billing Schemes - Creation of Fictitious Vendors or the Use of Shell Companies to Convert Monies

A common billing scheme is the creation of fictitious vendors or shell companies.

The perpetrator will create a fictitious vendor, usually a company owned by him or herself, and then have the fictitious bill the entity for goods or services it does not receive. Alternatively, the perpetrator can create a shell company to purchase goods or services, which are then marked up and sold to the employer through the shell. This scheme is most easily accomplished when one or few individuals maintain control over multiple functions and duties such as purchasing, selecting vendors, and receiving, and approving payments. Lack of adequate written cash disbursement procedures, such as requiring independent approval for disbursements over a particular amount, also heightens the risk of this scheme.

30.2. Third party vendor diligence is a useful prevention and detection technique. Such diligence should include:

Verification of the name and address of the new vendor by obtaining and maintaining on file copies of corporate records and other relevant documents evidencing its existence (and not simply a shell);

Obtaining credit references from reputed sources;

Requesting the vendor to furnish credit and other references establishing its identity; and

Checking the vendor address against the employee database to ensure that it does not match the known addresses of any employees or to determine whether any other relations exist between employees and the vendor. In addition, the auditor should be alert for addresses that are P.O. boxes. These should be considered as instant red flags of the existence of a fictitious vendor.

30.3. Once the new vendor has been approved, he or she should be entered into a master vendor database to which only a select few individuals have authority to enter into and change. These changes should be made in accordance with written procedures requiring proper authorization. An independent third party should periodically audit the database to ensure that the listed vendors are indeed still active and not being used to process fictitious invoices.

Once the company commences business with the vendor, an appropriate independent person should approve all purchase orders prior to being processed. In addition, adequate supporting documentation including an original invoice from the supplier, and a receipt to indicate that the product was delivered, should be requested and reviewed to support all cash disbursements.

The same person should not be able to both request and approve purchase orders. Likewise, only designated check signers should be able to disburse payment.

30.4. New accounts should also be monitored for some time for:

Increases in the amount or frequency of billings;

Variances from budgets or projections;

Discrepancies between the vendor's prices and those charged by other sources; and

Frequent or sizeable price increases by certain vendors with no explanation.

30.5. Billing Schemes - False Credits, Refunds, Rebates and Kickbacks

These fraudulent disbursement schemes require collusion between an internal employee and a third party to issue false rebates, discounts or credits. These schemes can occur with suppliers, as well as customers.

Deterrence and detection begin with the company's process for issuing and reviewing refunds, credits, rebates and discounts. Does the credit/refund/rebate process contain sufficient levels of review by independent supervisory authority? Do cash register employees possess authority to void their own transactions? Are only selected individuals authorized to offer rebates/discounts to vendors and customers? Do the appropriate people verify the rebate/credit transactions or are they merely "rubber stamped"? Is there adequate segregation of incompatible functions such as approval of vendors, maintaining the vendor master file, purchasing, processing of payments, and issuing and authorizing disbursements? Is there an adequate segregation of duties between individuals authorized to process checks and those in supervisory role? Is access to cash, checks, or purchase orders, shared by many employees?

30.6. Potential red flags for this scheme include:

Duplicate or multiple large amounts of refunds, credits or rebates, issued just under the review limit or in round numbers to the same vendor;

Excessive number of "voided" purchase or sales transactions for which no supporting documentation is found;

Unusual reconciling items or lack of timely resolution of reconciling items;

Large or numerous payments to particular vendors for which there is little or no supporting documentation or where the documentation contains discrepancies between the payment information and the back-up documentation;

Supporting documentation that contains anomalies such as invoices from several suppliers with different names but with the same address or which are signed by the same person or which return to a post office number; and

Sales contract specifications, purchase orders and invoices that are vague in nature;

30.7. The auditor can employ many of the procedures outlined in the fictitious vendor discussion above. In addition, the auditor should consider whether to:

Review outgoing credits and rebates to ensure that such payments are made in accordance with company rules and that any discount terms are accurately recorded;

Review and question supporting documentation for voided or refunded sales transactions;

Determine whether certain vendors are receiving preferential treatment with respect to credits and rebates; and

Inquire of personnel in the purchasing and cash departments whether they are aware of any vendors who maintain any sort of relationship with other personnel in the company.

Finally, as a note, whether searching for red flags or trying to actually detect the existence of this scheme, the auditor must always be cognizant of the existence of related parties whom the perpetrator may be using to commit this scheme.

30.8. Billing Schemes - Over Billing

An over billing scheme also involves collusion between an employee and third party. These generally involve extra illegitimate charges to a legitimate business expense or trade payable. This scheme is similar to false credits schemes and shares the same indicators. The auditor should be particularly wary of invoices carrying “extra” or “special” charges as well as discrepancies between the purchase order and invoice amount.

30.9. Billing Schemes - Pay and Return Scheme

Pay and return schemes involve employee perpetrators, who improperly pay a vendor or pay an invoice twice. The employee calls the vendor and requests return of the improperly issued or duplicate check. The employee then intercepts and converts the incoming check to his own use. This scheme is similar to unrecorded sales schemes and can be deterred and detected by techniques discussed in that section above.

30.10. Fraudulent Disbursements – Theft of Company Cheques

Cash larceny occurs when the perpetrator steals currency from the company. The theft can be of cash or its equivalent including cheques, CDs etc. Theft of company chequesis a common and easy way to accomplish cash larceny particularly when there is a clear lack of controls and segregation of duties in incompatible functions. Another basic but effective control is the maintenance of pre-numbered cheques. Thus, any check out of sequence will be easy to identify and investigated immediately.

30.11. In addition to the risks identified throughout this section, the auditor should be aware of the following factors that may facilitate the perpetration of this scheme:

Lack of adequate physical safeguarding of cash or incoming cheques;

Excessive amounts of voided cheques;

Numerous cheques payable to employees other than regular payroll cheques;

Excessive soft expenses (advertising, legal consulting etc.) or unexpected trends in expenses;

and

Cheques payable to “cash” or “bearer.”

30.12. Once the auditor has detected the possible existence of this scheme, there are various procedures he or she can perform to confirm this possibility. The starting point should be to review bank accounts established by company to ensure that they have been properly authorized and that only authorized personnel are drawing on them. Concurrent with such review, the auditor should also ensure that the company is maintaining policies and procedures which ensure that access to cash and bank accounts is maintained by select authorized employees and further that all assets including company cheques are adequately safeguarded and that access is restricted to a few select employees. The next step should be to perform reconciliations of various accounts looking for shortages or overages and reviewing bank reconciliations for old outstanding cheques that have not been followed up on. Other potentially helpful procedures include selecting sample cheques for review of various potential indicators including:

Evidence of alterations or other tampering;

Reviewing the endorsements to ensure that endorsements have been made by proper parties and cheques are deposited into authorized bank accounts; and

Reviewing endorsements for evidence of forgery, altered terms or other forms of tampering

30.13. Finally, if a perpetrator is going to steal cheques he will likely write them to either himself or to entities or individuals related to him or herself. Thus, the auditor should look for cheques with payments to “cash”, “bearer”, or unknown vendors. Similarly, the auditor should review the list of vendors for shell companies or for companies with no apparent business purpose to determine if the vendor is linked to employees in any manner. In this regard, any payments of excessive “soft” expenses to such vendors might be made with stolen cheques. The auditor should also review bank deposits to ensure that that the control total of cheques received matches the cheques withdrawn.

31. Payroll Fraud

Fewer and fewer companies pay employees in cash and many hire third parties to process payroll. Ironically, while these changes have simplified the processing of payroll, they also have increased the risk of payroll fraud.

Payroll fraud schemes generally occur in two major forms: the creation of fictitious employees and the padding of hours to cheat on time cards. Other payroll frauds include inflated overtime claims, the use of incorrect hourly rates, and overpayment of expenses or underpayment of deductions.

These schemes have different indicators and different means by which they are perpetrated. The intent of both is essentially the same; to defraud the corporation and steal from it.

31.1. Payroll Fraud - Ghost Employees

Ghost employee schemes involve payments to fictitious employees. Computerized payrolls, absent adequate controls are highly vulnerable to these schemes, as the computer does not know whether the employee is real or fictitious. A related scheme is to simply not remove former employees from the payroll.

Segregation of the duties of hiring, payroll processing and disbursement is essential to mitigating this risk. This helps to ensure that those in charge of processing employees into the payroll system do not get involved in disbursing cheques to fictitious employees they have created. Other significant controls include adequate procedures governing the hiring and firing process, and controls to ensure that new hires are adequately screened and that rigorous background checks are performed on them. Once entered into the payroll system, there must be checks and audits to ensure that the payroll, or individual records on it, cannot generate more than one payment for each period. Additionally, there should be checks to ensure that all payroll data is entered promptly, accurately and only once and in the proper accounting period. Finally, all employees who have been terminated or have otherwise left the firm should be promptly removed from the payroll system.

31.2. Procedures the auditor can perform to try to detect this scheme include:

Comparing a list of current and former employees to the current payroll list to search for and verify additions to payroll;

Matching master information from the payroll file with the organization’s personnel file to determine whether there are "ghost" employees on the payroll;

Comparing suspected employee’s social security numbers against list of valid numbers and test for duplicate employees on the entire payroll file (appending or joining payroll files if necessary.);

Reviewing direct deposit account numbers to look for duplicate deposits;

Randomly selecting employees and trace hours worked to time sheet (to ensure that all hours are approved by supervisor for hourly employees) and obtain employee file to ensure all proper documentation validating hiring of the employee is in place;

Ensuring that changes to payroll are adequately documented and supported;

Comparing the payroll file at two dates (i.e., beginning and end of a month) to determine whether recorded starters and leavers (hires and terminations) are as expected and if any employees have received unusually large salary increases;

Ensuring each employee's salary is between the minimum and maximum for his/her position or grade; and

Comparing holidays and sick leave taken to the limits for a particular grade or position and if there is a high rate of absenteeism for sickness analysing by department to identify problem areas

31.3. Payroll Fraud - Falsified Hours

Cheating on hours worked is a very easy way to steal from an employer, as it is very difficult to validate the hours an employee spends on a given assignment. To guard against this practice, an employer must establish strong internal controls that encompass some or all of the following procedures:

Maintain checks to ensure that all payroll data is entered promptly, accurately and only once and in the proper accounting period;

Require that all sales commission claims be made in writing;

Ensure that all claims are checked to vouchers and any other supporting documentation prior to authorisation;

Establish procedures to check claims to ensure that the correct reimbursement rates have been used;

Establish procedures to ensure that all alterations to claim forms are countersigned; and

Establish procedures to ensure that signatures of authorised counter-signatories are checked before payment is made.

31.4. The auditor in turn can attempt to detect this by:

Reconciling time cards/sheets (with approved supervisor signature and employee signature) to pay cheque; and

Recalculating commissions by testing sales invoices, back to sales orders, shipper, and customer receipt.

32. Sham Related Party Transactions

32.1. Sham related party transactions are transactions between related parties, where either little or no consideration is given for the product or service. The existence of related party transactions does not meet that there be persuasive evidence of an arm's length arrangement. Sales transactions should stem from express or implied contracts and represent exchanges between independent parties at arm's-length prices and terms. Accordingly, arms-length transactions cannot be achieved in those situations, where the parties are related or where one party can exercise substantial control over the other.

32.2. Related party transactions carry the presumption that one or both parties have received a benefit that they would not have otherwise received had the transactions been truly arm's length.

Transactions between related parties are often difficult to audit, as these transactions are not always accounted for in a manner that communicates their substance and effect with transparency. The possibility of collusion always exists, given that the parties arerelated. Internal controls, moreover, might not identify the transactions as involving related parties.

32.3. An auditor may encounter related parties that are known by some members of the company; however, the relationships are not properly disclosed in the books and records. The auditor should inquire as to outside business interests and then try to determine whether they are properly disclosed, and the volume of transactions, if any, that are occurring between the entities.

Auditors should also focus on the relationship and identity of the other party to the transaction and whether the transaction emphasizes form over substance. Common indicators of such related party, sham transactions include but are not limited to:

Borrowing or lending on an interest-free basis or at a rate of interest significantly above or below market rates;

Selling real estate at prices that differ significantly from appraised value;

Exchanging property for similar property in a non-monetary transaction;

Loans with no scheduled terms for when or how the funds will be repaid.

Loans with accruing interest differing significantly from market rates;

Loans to parties lacking the capacity to repay;

Loans advanced for valid business purpose and later written off as uncollectible;

Non-recourse loans to shareholders;

Agreements requiring one party to pay the expenses on the other's behalf;

Round tripping sales arrangements (seller has concurrent obligation to purchase from the buyer);

Business arrangements, where the entity pays or receives payments of amounts at other than market values;

Failure to adequately disclose the nature and amounts of related party relationships and transactions as required by Accounting Standards;

Consulting arrangements with directors, officers or other members of management;

Land sales and other transactions with buyers of marginal credit risk;

Monies transferred to or from the company from a related party for goods or services that were never rendered;

Goods purchased or sent to another party at less than cost;

Material receivables or payables from to or from related parties such as officers, directors and other employees;

Discovery of a previously undisclosed related party;

Large, unusual transactions with one or a few other parties on or at period end; and

Sales to high-risk jurisdictions or jurisdictions where the entity would not be expected to conduct business.

If related party transactions are detected or suspected, the auditor should consider further inquiry, including:

Conducting public records searches/background investigations on customers, suppliers and other individuals to identify related parties and confirm legitimacy of business;

Performing data mining to determine whether transactions appear on computerized files;

Performing document review of identified transactions to obtain additional information for further inquiry;

Searching for unusual or complex transactions occurring close to the end of a reporting period;

Searching for significant bank accounting or operations for which there is no apparent business purpose;

Reviewing the nature and extent of business transacted with major suppliers, customers, borrowers and lenders to look for previously undisclosed relationships;

Reviewing confirmations of loans receivable and payable for indications of guarantees;

Performing alternative procedures if confirmations are not returned or returned with material exceptions;

Reviewing material cash disbursements, advances and investments to determine if the company is funding a related entity;

Testing related party sales to supporting documentation (i.e., contract and sales order) to ensure appropriately recorded;

Discussing with counsel, prior auditors and other service providers the extent of their knowledge of parties to material transactions; and

Inquiring about side agreements with related parties for right of return or contract cancellation without recourse

33. How to detect premature Revenue Recognition

33.1. Technique used to detect premature revenue recognition are textbook audit procedures. The trick is to apply the proper degree of professional skepticism in interpreting the results. A lack of diligence in employing reasonable and necessary techniques like the ones described below can easily lead to an audit failure.

33.2. If one employee processes the same transaction from beginning to end, premature revenue recognition is easier to accomplish. Adequate internal controls involve the following

segregation of duties: order entry, shipping, billing, accounts receivable detail and general ledger. Even adequate internal controls can be overridden by management, so be alert to the indicators that controls are not being followed. If sales or shipping invoices are out of a numerical sequence, check to see if the documentation has been hidden.

33.3. In premature revenue recognition cases, goods are often billed before they are actually shipped, so quantities of goods shipped will not reconcile to the goods billed. Check the reconciliations for accuracy. Select a sample of sales transactions from the sales journal, obtain the supporting documents and:

(a) Inspect the sales order for approved credit terms.

(b) Compare the details among sales orders, shipping documents and sales invoices for inconsistencies.

(c) Compare the prices on sales invoices against published prices.

(d) Re-compute the extensions on sales invoices.

33.4. When merchandise is shipped early, the shipping costs near the end of the accounting period could be higher. Compare shipping costs to previous periods for reasonableness. Moreover, conduct a standard cut-off test by selecting invoices from the end of the previous period and those from the beginning of the next period. Examine the invoices to make sure they are recorded in the proper period. When in doubt, verify major sales through confirmations or by telephone. Look for discrepancies in sales records.

By recording expenses belatedly, a company can fraudulently inflate its net income. (A variation of this technique is failing to record returns and allowances in the proper period).

33.5. Most frequently, accounts payable personnel are told to hold all unpaid bills until the beginning of the next accounting period. Often, the unpaid invoices are simply secreted in a desk or filing cabinet, out of sight of the auditors. Ask those responsible for recording liabilities whether they have been instructed to hide unpaid bills. Document the inquiry in your workpapers.

34. Remember the Motive

34.1. To determine how much pressure is on management to show high levels of earnings, find out whether the company is attempting to raise additional funds through stock issues or borrowings. If these risk factors or similar others are present, recognize this reality. Companies can and do significantly influence income, expense and profits by manipulating the cut-off time. As an auditor, considering this fact as a part of the risk equation will help keep you from being fooled by fake cut-offs.

34.2. Ask the Right Questions

34.2.1. A third lesson is specific to auditors of manufacturing, wholesale and retail firms—those with a loading dock. Every inventory item eventually finds its way to the loading dock,

either coming or going. As a result, key shipping and receiving personnel know if financial shenanigans are occurring in inventory. For example, the warehouse becoming too full of junked merchandise and that off-site storage had to be rented. The loading dock employees knew shipping documents had been backdated and that consignment merchandise had been counted as sales.

In a thorough audit involving inventory, the auditor should ensure that he or she spends enough time on the loading dock. In addition to the normal audit steps, the auditor should make diligent inquiries. Asking tough questions is not hard if you do it right. Here is an example: "Mr. Warehouseman, as you know, part of my job as an auditor is to detect fraud. As a result, I will need to ask you and other people I talk to some specific questions about fraud and abuse. Do you understand?"

When you have broken the ice, ask the following:

Has anyone in the company ever asked someone on the loading dock to misstate the amount of merchandise the company ships or receives?

Are you aware of anyone in the company asking someone on the loading dock to destroy, conceal, backdate or postdate documents?

Has anyone in the company asked you to do anything else you thought was illegal or unethical with respect to your job?

If you receive answers that make you pause, assess the risk of material financial statement fraud in light of other relevant information. Don't be reluctant to ask penetrating (but non-accusatory) questions. You may be surprised at what people will tell you and the mere fact that employees understand that auditors are looking for fraud can be a significant deterrent.

35. The Acid Test

Nonetheless, before the auditor signs off on the engagement, he or she should use an acid test to evaluate the analytical review, reflecting on this question: If management was attempting to conceal a material financial statement fraud, where would it show up? By thinking of fraud as a "worst-case" scenario, you will find your focus quickly sharpen and the degree of your professional skepticism should rise.

The auditor who uses these techniques will find they can pay big dividends. Any legitimate client will appreciate your anti-fraud efforts. After all, fraud costs money. And if a client resists or restricts your efforts to detect and deter fraud, that should raise a big red flag.

36. Opportunities

The following opportunities may result into financial statements frauds:

(a) Absence of oversight by the Board of Directors or by Audit Committee;

(b) Weak or non-existent Internal Control methods;

(c) Where financial statements require significant judgement;

(d) Significant related party transactions;

(e) Highly complex transactions and also complex organisational structure.

37. Detecting Financial Statement Frauds:

37.1 Looking back at Enron, perhaps the company best known for committing accounting fraud, one can see the different methods that were utilized so as to fraudulently improve the appearance of its financial statements. Through the use of off balance sheet, the firm continued to hide its liabilities and inflate its earnings.

37.2. In 1999, limited partnerships were created for the purpose of purchasing Enron shares, as a mean of improving performance of its stock. That year, the company returned 56% to its shareholders, which was followed by another 87% appreciation at the onset of the new millennium. As Enron's aggressive accounting practices and financial statement manipulation began to spiral out of control, the scandal was eventually uncovered by the complex accounting fraud such as that practiced at Enron is usually extremely difficult for the average retail investor to discover. However, there are some basic red flags that help during the preliminary stages of the investigation. Despite passage of SOX (Sarbanes-Oxley), financial statement fraud remains too common an occurrence, often damaging people's retirement and educational savings.

Being first on the scene to uncover a fraudulent company can be very lucrative from a short seller's perspective and can be rather beneficial to a skeptical investor, who is weighing in the overall market sentiments?

38. Financial Statement Fraud Red Flags

38.1. Financial statement red flags provide a general overview of the warning signals investors should take note of. These red flags do not necessarily indicate an undoubted occurrence of financial statement fraud, but merely a signal that further in-depth investigation must be carried out, so as to assess the validity of the corporate documents.

Creditors would find such information useful for ensuring that the loans are not provided to firms operating with high and increased amount of risk.

38.2. Investors, on the other hand, may want to take note of the following factors to discover new shorting opportunities. Government regulators, however, aim to catch and punish fraud to ensure the transparency and reliability of the financial markets.

38.3. Five basic types of financial statement fraud exist:

Fictitious sales (Goods not yet sold, recorded as sales)

Improper expense recognition (meaning that not in accordance with applicable Accounting Standards)

Incorrect valuation of Assets (Not charging correct value of depreciation in the revenue statements)

Hidden Liabilities (Means Liabilities not reflected at their true and fair value), and

Unsuitable or inadequate disclosures in the Financial Statements.

39. Misappropriations

39.1. One of the most serious forms of financial statement fraud is when statements are altered so as to mask the theft or embezzlement. This can be done in a number of ways, such as (a) through double-entry bookkeeping or (b) the inclusion of fictitious expenses. In this case, the fraud is generally committed for purely personal gains, and not through an interest in altering public perception of the company,

39.2. Another way of financial statement fraud could be in the form of making Assets appear as more valuable than they actually are. This is done either by adding fictitious assets and charging lower amount of depreciation. Although the entries in the financial statements may be true, the appraisals that led to these statements being written are incorrect. For example, if an oil company deliberately appraises a non-producing well as worth the same as one that produces oil, and include this valuation on its financial statement, this is a form of fraud.

40. Overstatement of Revenue

One of the most basic forms of financial statement fraud is the overstatement of revenue. In this form of fraud, a company states that it took in more money in a certain period of time than was the case. This may be done for several reasons, all related to creating the perception that the company is worth more than it is.

40.1. Recording Uncertain Sales: Another form of financial statement fraud is to record sales that have not yet gone through as sales that have already been transacted. This can take several forms, including sales that are currently being negotiated or sales that are expected for the next quarter. This form of fraud is closely related to the recording of false revenues. Like false revenues, this form of fraud is designed to make the company appear more profitable than is the case.

40.2. Concealment of material facts: Concealment of Material facts, which have bearing on Financial Statements, is another form of fraud, wherein certain liabilities, expenses or even other critical disclosures, that could impact the financial results of the company, are not disclosed in the financial statements. For example, if the company took on a number of liabilities, such as by taking out a loan or issuing debt, this will generally need to be recorded. By keeping such disclosures off the financial statements, the company looks in better financial shape, than is the case.

41. How to prevent financial statements frauds

41.1. A long time trusted employee has confessed having misappropriated company funds.

Unfortunately, business owners are often engrossed in managing employees, customer service and putting out daily fires that a majority of the financial responsibilities are entrusted to someone else. However, once an entrepreneur has become the victim of fraud, he searches for answers to prevent the situation in the future. A strong system of internal controls helps companies deter employees from committing fraud. Following are the some steps that need to be taken in the matter:

Step 1

41.2. Educating the Management about different indicators of fraud. According to the Association of Certified Fraud Examiners, financial statement fraud involves intentional publishing of false information in any portion of a financial statement.

To prevent fraudulent activities, management must implement internal controls, or structure, and know what situations to look for.

Individuals commit fraud when (i) under situational or financial pressure, (ii) when the opportunity to commit fraud is present and (iii) when the perpetrator easily rationalizes the fraudulent activity.

Step 2

41.3. Segregation of accounting functions:

One of the main factors of an effective internal control system is Segregation of Duties. The opportunity to commit fraud, is reduced when accounting functions are separated. The act of segregating duties separates the recordkeeping, authorization and review functions in the accounting process.

To segregate duties, involve more than one person in the financial statement preparation process. Therefore, for fraud to occur two employees must collude to perpetrate the crime.

Step 3

41.4. Establish a strong control environment:

Establishing a strong control environment, also known as a strong tone at the top, involves enlisting management to demonstrate ethical behaviour. It may be noted that whatever tone management sets, will have a trickle-down effect at the bottom level. A strong tone is developed by establishing and complying with a written set of policies and procedures. The policies must be concise and must include consequences when procedures are disobeyed. In addition, one of the easiest ways to establish a strong moral tone for an organization is to hire morally sound employees.

Step 4

41.5. Initiate Annual examinations of Financial Statements:

41.5.1. Annual audit of the financial statements by an external and independent party. In many

cases, management is the party to the frauds. Management may feel pressure to meet financial goals for the company or may receive incentives, if certain goals are achieved.

41.5.2. To help prevent management from engaging in adjustments to the financial statements, it is desirable to engage an independent party to examine financial statements on an annual basis. Engaging an auditor to perform a financial statement review or audit, deters employees from knowingly presenting incorrect financial statements.

Effectively spotting these fraudulent disclosures involves keeping an open eye for the most common financial statement fraud red flags:

An eye on the accounting anomalies, for example growing revenues not supported by corresponding growth in cash flows.

Sales are much easier to manipulate than cash flow, but the two should move more or less in tandem over time.

Reporting of consistent growth in sales, whereas other established competitors are experiencing periods of weak performance. This situation should work as eye opener to the Management. However, actual reasons need to be looked into, whether the consistent growth in the sales is on account of high quality of products manufactured by the company supported with efficient after sales service. In such as a situation, this is called as growth due to efficient business operations rather than any fraudulent activity.

A rapid but unexplainable rise in the number of day's sales in receivables in addition to growing inventories. This suggests rise in obsolete goods for which the firm has been recording fictitious future sales.

A significant surge in the company's performance within the final reporting period of fiscal year. The company may be under immense pressure to meet analysts' expectations.

The company maintains consistent gross profit margins, while its industry is facing pricing pressure. This can potentially indicate failure to recognize expenses or aggressive revenue recognition.

A large build-up of fixed assets: An unexpected accumulation of fixed assets can flag the usage of operating expense capitalization, rather than expense recognition.

Depreciation methods and estimates of assets' useful life that do not correspond with the industry standards. An overstated life of an asset will decrease the annual depreciation expense.

A weak system of internal control. Strong corporate governance and internal controls processes minimize the likelihood that financial statement fraud will go unnoticed.

Outsized frequency of complex related-party or third-party transactions, many of which do not add to any tangible value.

The firm is on the brink of breaching their debt covenants. To avoid technical default, management may be forced to fraudulently adjust its leverage ratios.

The auditor was replaced, resulting in a missed accounting period. Auditor replacement can signal a dysfunctional relationship while missed accounting period provides extra time to "fix" financials.

A disproportionate amount of managements' compensation is derived from bonuses based on short term targets. This provides incentive to commit fraud.

42. Financial Statement Fraud Detection Methods

42.1. Spotting red flags could be extremely challenging, as corporates engaged in the fraudulent activities, would make all possible attempts to portray good image about the financial stability and normal business operations.

42.2. Vertical and horizontal financial statement analysis introduces a straight-forward approach to fraud detection. Vertical analysis involves taking every item in the income statement, as a percentage of revenue and comparing the year-over-year (YoY) trends that could be a potential flag cause of concern. A similar approach can also be applied to the balance sheet, using total assets as the comparison benchmark, to monitor significant deviations from normal activity. Horizontal analysis also implements a similar approach, whereby financial information is represented as a percentage of the base years' figures. Likewise, unexplainable variations in percentages can serve as a red flag requiring further analysis.

42.3. Comparative ratio analysis also allows analysts and auditors to spot discrepancies within the firm's financial statements. By analysing ratios, information regarding day's sales in receivables, leverage multiples and other vital metrics could be determined and analysed for any inconsistencies.

42.4. A mathematical approach, evaluates certain ratios to determine the likelihood of earnings manipulation. Asset quality, depreciation, gross margin, leverage and other variables are factored into the analysis.

42.5. Similar to most other ratio-related strategies, the full picture can only be accurately portrayed once the multiples are compared to with the industry standards and also with specific firm's historical average.

Having proper knowledge of the red flags so as to avoid companies indulging into unscrupulous accounting practices is a useful tool to ensure safety of your investments.

42.6. Other measures or steps to be taken are 10 considerations for detecting or preventing fraudulent financial reporting:

1. Developing a right culture at the top or senior management level: (i.e., tone up at the top). Probably the most important deterrent to financial fraud is that senior management creates a culture in the business that send a message amongst all employees that any kind of dishonesty will not be tolerated. Top Management need to go on record that they expect to work be carried out in an ethical environment and expect employees to

conduct themselves in an ethical manner.

2. Establish and promote an effective whistle-blower program. Providing the ability for employees to anonymously report questionable practices, which could lead to uncovering frauds before it affects financial reporting systems. Having an effective whistle-blower program in place can deter fraud before it starts.

3. Questioning financial results that are always on target. No business is immune to market forces and fluctuations, and those fluctuations should be reflected in financial results. If the numbers are always on target, it may mean the financial information is being manipulated.

4. Questioning when there are changes in auditor. All of the changes happened in either the year of the fraudulent reporting or in the year just prior.

5. Have skeptics on the Board of Directors. Having a Board of Directors and specifically members of the Audit Committee, who have knowledge about the business and the sector and willing to question when things seem outside the norms, could be a significant deterrent to fraudulent financial reporting.

6. Raising question when there are extraordinary or complex transactions, especially question extraordinary transactions, either positive or negative, that offset results from operations. One significant gain that would offset a bad year of results may be used to improve the bottom line.

7. Analysing Accounts Receivables, more particularly, to unearth any instance of revenue manipulation, a common form of financial fraud, will often affect receivable balances. Investigation of outlier activity in receivables, basis for uncollectible accounts, and receivable statistics in comparison to industry standards could help in identification of potential financial reporting problems.

8. Again raising questions when cash flows do not match the growth in the revenue. Again because revenue manipulation is among the most common forms of financial fraud, management should be able to justify if a revenue increase is not accompanied by a corresponding increase in cash flow.

9. Analysing major swings in the assets or liabilities. Manipulation of revenues or expenses normally involve unexplained swings in the assets and liability balances. There should always be a logical explanation for significant changes in balance sheet accounts.

10. Continue to educate yourself and urge others to do the same. Accountants, management, employees, investors, and directors need knowledge to combat fraudulent financial reporting. By knowing the “red flags” of fraud and understanding the difference between aggressive but acceptable accounting and abusive and prohibited accounting, individuals can stop fraud before a company and its stakeholders are

harmed by fraudulent financial information.

43. Magnitude of Fraud Losses:

43.1. Every organisation, whether large or small, is, in general prone to frauds. On a number of occasions over the past few decades, major public companies have experienced financial reporting frauds, resulting into turmoil in the capital markets, loss of shareholders value, and, in some cases, even the bankruptcy of the company itself. Although, it is generally accepted that the Sarbanes-Oxley Act (SOX) has improved corporate governance and decreased the incidence of frauds, recent studies and surveys indicate that investors and management continue to have concerns about financial statement frauds.

44. Consequences of Fraudulent Reporting

44.1. Fraudulent financial reporting could have significant consequences for the organisation, investors and its other stakeholders, it as well as badly impacts the public confidence in the capital markets and financial reporting process. They tend to lose their faith in the accounting and auditing system.

44.2. Periodic high-profile cases of fraudulent financial reporting also raises concerns about the credibility of the financial reporting process and calls for several questions about the roles of management, their integrity, auditors, regulators, and analysts, among others. Moreover, corporate fraud impacts organisations in several areas viz., financial, operational and psychological. While the monetary loss owing to fraud is significant, the full impact of fraud on an organisation could be staggering. In fact, the loss of reputation and customer relations could have devastating effects.

44.3. When there are instances of fraudulent financial reporting, they give rise to serious consequences. The resultant damage could be severe and widespread, with a sometimes devastating “ripple” effect. Those affected may range from the “immediate” victims (the company’s investors and other stake holders) to the more “remote” (those harmed when investor confidence in the stock market is shaken). Between these two extremes, many others may be affected: “employees” who suffer job loss or diminished pension fund value; “depositors” in financial institutions; the company’s “underwriters, auditors, attorneys, and insurers”; and even honest “competitors”, whose reputations suffer for their association with the company or enterprise.

44.4. As frauds could be perpetrated by an employee (within the organisation) or by those from the outside, therefore, it is important to establish and have an effective “fraud management” programme in place to safeguard the assets and image of the organisation. Thus, the process of prevention and quicker detection of fraudulent financial reporting, must start with the entity that prepares financial reports.

44.5. Given the current state of the economy and recent corporate scandals, fraud is still a topmost concern for corporate executives. In fact, the sweeping regulations of Sarbanes-

Oxley, designed to help prevent and detect corporate frauds, have exposed fraudulent practices that have gone undetected in the past. Additionally, more corporate executives are paying fines and serving prison time than ever before. No industry is immune from frauds and the negative publicity, which swirls around them. The implications for management are clear: every organisation is vulnerable to fraud, and managers must know how to detect it, or at least, when to suspect it.

44.6. Methods for detection of Financial Frauds mainly rely on financial statistics, although recent research suggest that even linguistic or vocal cues may also be useful indicators of deception. Tools developed based on financial numbers, linguistic behaviour, and non-verbal vocal cues have demonstrated the potential for detecting financial frauds. However, the quality of performance of such tools is considered to be poorer than expected and thereby limiting their use on a stand-alone basis to help identify companies for further investigation.

Financial Statement frauds have become quite rampant in the current times, when a number of financial frauds have been unearthed and reported. These financial frauds run into millions of rupees and have revealed complete absence of surveillance and disregards to the financial controls and applicable accounting standards. These frauds have been perpetrated mainly by the key managerial persons for achieving certain financial benefits.

45. Effects of the Financial Statement Frauds

(i) It reduces the reliability, quality, transparency and integrity of the Financial Reporting Process;

(ii) Jeopardises the integrity and reliability of the auditing profession and erodes public confidence in the accounting and auditing profession;

(iii) Reduces Investors' confidence in the Capital Markets and makes Capital Markets less efficient;

(iv) It adversely effects Nations economic growth and prosperity;

(v) Raises serious doubts about the financial statement audit;

(v) Destroys career of the employees involved in the financial statement frauds;

(vi) Causes bankruptcy or substantial economic losses to the company involved in the financial statement frauds

46. Auditor Responsibilities

46.1. Normally, the risk of not detecting material misstatements due to fraud is higher than not detecting misstatements due to error. This may occur because perpetrators of fraud might have used carefully designed methods of forgery, transactions recording, and misstatements. In addition, several persons may collude to conceal the fraud. The risk of management fraud not being detected is usually greater than employee fraud, because management has a greater opportunity to override internal controls and manipulate accounting information.

46.2. Developing sense of a Professional Skepticism

46.2.1."Skepticism refers to an attitude of raising questions, when there are reasons to doubt and also being alert to conditions that might indicate possible misstatement due to frauds or errors, and making critical assessment of audit evidences."

46.2.2. Risk of material misstatement at the financial statement and assertion levels will affect the degree of the auditor's professional skepticism. While an auditor will always maintain professional skepticism, higher assessed levels of risk of material misstatement should result into higher levels of professional skepticism. For example, when risk of material misstatement is high, an auditor should request supporting documentation to corroborate management's responses to inquiries.

46.3. Engaging in Team Discussion

In the engagement team's planning and brainstorming meeting, the engagement leader (e.g., partner, sole proprietor or practitioner) should facilitate a discussion about possible misrepresentation in the financial statements and misappropriation of assets. The engagement team should hold this discussion by disregarding beliefs and knowledge of the honesty and integrity of entity management and employees. Particularly for recurring audits, familiarity with the honesty and integrity of reporting entity personnel may inadvertently lead to a decrease in an auditor's professional skepticism. Compliance with the specific requirements of this statement, paired with audit firm's quality control system, will provide safeguards to prevent this possibility.

46.3.1. Some of the matters the engagement team should discuss at meetings include:

All internal and external factors that could be part of the "fraud triangle":

Incentives and pressures to commit fraud.

Opportunities to perpetrate fraud.

Rationalizations for committing fraud.

Possibilities and risk of management override of controls.

Circumstances that might cause management to manage, manipulate, or misstate financial information.

How professional skepticism should be maintained during the audit and how team members should respond to assessed levels of risk of material misstatement.

46.3.2. Auditors should follow up fraud indicators by looking for:

Transactions lacking all required supporting documentation;

Numerous disbursements approved by one particular employee to a particular vendor which are just below the employee's spending authority or which are for large even amounts or which are made on unusual dates such as weekends and holidays;

Invoices which do not match with the original purchase order and if applicable the original sales contract;

Multiple payments to the same vendors in the same period by the same employee usually under the employee's spending limit;

Excessive "soft expenses" such as consulting fees, sales commissions, and advertising where there are no tangible products attached to the payable, paid to the same vendor by the same or few employees;

Checks made to "cash" or "bearer" for alleged services or products received;

Suspect endorsements on checks; and

Checks with more than one endorsement, checks payable to businesses or individuals that were cashed and not deposited and checks endorsed by individuals.

46.3.3. Computer assisted auditing programs are available for many of these indicators.

The auditor should compare the master vendor database against the prior year's database. The auditor should inquire into the selection and approval process of new vendors. Further, the auditor should match the checks issued against the master vendor database, and investigate any payments to vendors who are not in the master database.

47. Forensic Auditing Techniques

The auditor should perform the following techniques, when investigating revenue recognition allegations:

Inquire of management and other relevant personnel about the factors which have led the auditor to believe the scheme exists;

Perform substantive analytics designed to detect the fraud being investigated; and

Perform substantive testing to determine whether there is some evidence to support the existence of such a scheme or lack of evidence to support the validity of a transaction. Such substantive procedures include but are not limited to:

Request and review documents such as contracts and support for invoices and deliveries;

Confirmation with customers to the existence of accounts receivable and the amount of consigned goods;

Possible public records/background research/site visits conducted on customers/third parties to verify existence of the entity being billed;

Analyzing journal entry activity and supporting documentation in certain accounts, focusing on round dollar entries at the end of periods;

If entries are accruals, obtaining support for the reversal and confirming the proper timing of the entries.

The following general indicators can often alert the auditor or auditor as to the potential existence of premature revenue recognition:

Unexplained change in recognition policies;

Unexplained improvements in gross margin;

Increasing sales with no corresponding increase in cash from operations;

Reported sales, revenue or accounts receivable balances which appear to be to high or are increasing too fast;

Reported sales discount, sales returns or bad debts expenses which appear to be too low;

Large, numerous or unusual sales transactions occurring shortly before the end of the period;

Large amounts of returns or credits after the close of a period; or

Inconsistent business activity –

Increased revenues with no corresponding increase in distribution costs or

Increased revenues with no offsetting increase in accounts receivable.

The use of analytics should also not be overlooked as a means of detecting frauds. Analytical procedures and relationships the auditor can perform or review to determine whether revenue is being recognized prematurely include:

Comparing current period financial statement amounts with amounts with those from prior periods and inquiring as to significant changes, in accounts between periods, if there are significant changes;

Reviewing balances in revenue related accounts for any unusual changes;

Calculating the percent of sales and receivables to the total balance sheet in the current period, comparing it with prior periods and inquiring of any unusual changes;

Reviewing the statement of cash flows to determine if cash collected is in proportion to reported revenues;

Reviewing sales activity for the period and take note of any unusual trends or increases such as increases towards the end of the period;

Significant or unusual or unexplained changes in the following ratios:

Increases in Net Profit Margin (Net Income/Total Sales);

Increases in Gross Profit Margin (Gross Profit/Net Sales);

Increases in the Current Ratio (Current Assets/Current Liabilities);

Increases in the Quick ratio (Cash and Receivables and Marketable Securities/Current Liabilities);

Increases in the Accounts Receivable Turnover (Net Sales/A/R);

Increases to Days Sales Outstanding (A/R Turnover/365);

Increases in Sales Return Percentages (Sales Returns/Total Sales);

Increase in Asset Turnover (Total Sales/Average Total Assets);

Increases in Working Capital Turnover (Sales/Average Working Capital);

Decrease in A/R Allowance as a % of A/R (Allowance/Total A/R); and

Decreases in the bad debt expense or allowance accounts.

47.1. Of course, good interviewing and sound analytics will not substitute for having a good understanding of the client's business. Even seasoned auditors have been misled and thought revenue to be appropriate, because they did not fully understand the business. Thus, after all the analytics and interviews, the auditor must ask him or herself whether the information and results obtained make sense in light of the client's industry and business. The auditor should also, to the extent applicable, benchmark performance results against other companies in the same industry.

47.2. The auditor should also make broad inquiries of non-financial personnel such as:

Shipping department personnel:

Were shipments earlier than normal for customers?

Is inventory stored in the warehouse documented as shipped?

Was there inventory shipped to addresses other than customer sites?

Were there any adjustments to shipping dates?

Whether there exists consigned goods and their location.

Sales force personnel:

Are shipments of any products designed to arrive ahead of the customer's required delivery date?

Do sales personnel pick up product and deliver to customers?

Are there sales personnel with excessive "samples"?

Do sales personnel have free reign in access to the warehouse?

Warehouse personnel:

Are there any misstatements in the amount of merchandise the company ships or receives?

Has there been destruction, concealment, predating, or postdating of shipping and/or inventory documents?

Has there been an acceleration of shipments prior to month or year-end?

Have there been shipments to a temporary or holding warehouses prior to final shipment to the customers' premises?

Are there any other unusual, questionable, or improper practices?

47.3. Additional audit procedures include:

Comparing the purchase order date with the shipment date;

Determine whether sales personnel are paid commissions based on the sale of product or upon collection;

Inquiring of outside related business interests of key/sales personnel that may be suspected in an improper revenue recognition scheme;

Performing public records searches on certain entities and individuals;

Determining whether shipments have been made to these outside business interests;

Reviewing amounts and trends of shipping costs at or near the end of a period even to legitimate customers;

Reviewing rate of returns;

Inspecting shipping documents for missing, altered or incorrect information; and

Reviewing customer complaint logs or e-mail correspondence for complaints of shipments of goods prior to the customer's readiness to accept.

48. Fraud Risk Assessment Procedures

48.1. Discussions with management and others included in the auditor's risk assessment procedures may include:

Management's internal control risk assessment and monitoring processes.

Management's communication with persons charged with governance regarding risk assessment, monitoring, and any planned corrective actions.

Management's communication of business practices and ethical behaviour to employees.

Management's and persons-charged-with-governance's knowledge of alleged, suspected or actual fraud.

Persons-charged-with-governance's oversight of management's processes and internal controls for identifying and responding the risks of fraud.

Results of the auditor's analytical procedures and any unusual or unexpected relationships that may be indicative of fraud.

49. Third Party Fraud?

49.1. This is a fraud committed by people outside an employee employer relationship. They can be committed against individuals, businesses, companies, the government or any other entity. Third party frauds are not as common as occupational frauds, but on average each fraud is for a larger amount.

49.2. Some third party frauds are not meant to remain hidden forever. Some only remain hidden long enough for the fraudster to make their get-away. The fraudster may not care if the fraud is eventually discovered as they do not have a continuing relationship with the victim and they cannot be found.

50. Lessons to be learnt

50.1. The role of auditing was created so that an independent person could look behind the reality of the financial statements and discover, whether they were accurate. While this is not an exact science and the cost of an audit could be huge. As costs constraints make test sample sizes smaller, the chances that mis-statements would slip through the examination increases.

50.2. Financial statement frauds are committed within the business, not on the business. The best way of preventing or detecting these frauds is a strong internal and independent audit function. Internal and independent can seem contradictory, but it is an idea that must become a reality. Some of these frauds have originated from the pressure to get short term results. If the consequences of not getting the results are too great, improper or illegal behaviour will increase. Corporate ideals have a large role to play in deterring these activities, by making them unnecessary.

50.3. Of all the fraud schemes perpetrated in today's time, financial statement fraud seems to get the least air time. That makes no sense, as financial statement fraud happens to be one of the most costly types of fraud. The problem is that involved parties, both inside and outside the company, rely on the information provided in the financial statements. They assess the financial results and make predictions and decisions about the future of the company based on those results.

50.4. Financial statements are the measuring stick that numerous parties use to assess the financial health of a company. Falsified financial statements can mean only one thing – those assessments are faulty.

50.5. Asset misappropriation schemes are easy to understand and recognize. They include the direct theft of money, inventory, equipment, or other company assets. Most everyone can relate to the theft of property and money, and the results of such theft are tangible.

But financial statement fraud is an ugly fraud. Its methods are complex and often not understood by the average consumer or investor. And its results often aren't tangible to the average person, unless we're talking about a famous fraud like Enron.

51. The Perpetrators

51.1. Financial statement fraud is almost always perpetrated by upper management or company owners. Executives are entrusted with entire companies. They have access to nearly all data and employees, and they can exploit this access to commit and fraud and cause the fraud to be concealed. The power the executive has by virtue of her or his position in the company is closely linked with the high cost of financial statement fraud. Power and access within a company make it possible for larger frauds to be committed and covered up.

51.2. The breach of trust when an executive is involved in fraud is huge. How can lower-level employees be expected to act ethically when those in charge of the company lack ethics of their own?

51.3. Different types of Frauds, their perpetrators and victims:

Types of Frauds	Perpetrator	Victim	Explanation
1. Embezzlements	Employees	Employer	Employees directly or indirectly steals.
2. Management Frauds	Top Management	Stakeholders, Lenders and others who rely on Financial Statements	Mis-Statement in the financial statements by the Top Management.
3. Investment Scams	Individuals	Investors	Investors are deceived and advised to invest their funds in fraudulent schemes.
4. Vendors fraud	Vendors	Buyers	Overcharging for goods or no delivery of the goods which has been fully paid.
5. Customers fraud	Customers	Buyer Organisation	Customers deceive sellers.

52. The Methods

52.1. One of the most innocent-sounding terms used to describe financial statement fraud is “earnings management.” Such a phrase minimizes the seriousness of the crime. “Management” almost makes it sound like something good.

But earnings management isn’t a noble effort. It is, in fact, financial statement fraud. The degree and seriousness can vary, but it is fraud nonetheless. It is the purposeful manipulation of account balances in order to make the financial statements conform to some predetermined template.

52.2. Especially with public companies, there are expectations related to the financial results, and executives may alter numbers to conform. Earnings management (financial statement

fraud) means that management played games with the numbers, shifting revenue or expenses from one period to the next, or inflating assets or underreporting liabilities.

52.3. In addition to the opportunity to manipulate revenue, expenses, assets and liabilities, there are other forms of financial statement fraud that are gaining in popularity. Schemes include the misuse of reserves, often referred to as using reserves as “cookie jars” to shift income and expenses between periods depending upon the company’s “need” for the financial statements to fall within certain parameters.

52.4. The misapplication of accounting rules is another opportunity for financial statement manipulation. Executives may deliberately incorrectly apply accounting rules in a way that enhances the company’s financial results.

52.5. One of the simplest ways to manipulate financial statements is through the omission of information. There are rules regarding explanations and disclosures that must accompany financial statements. Without that additional information, the financial statements themselves might easily be misinterpreted. Deliberately omitting necessary information from the notes to the financial statements is a simple, but effective, way to tender misleading financials.

53. The Results

53.1. Financial statement fraud can have an impact on any person or organization that has a financial interest in the success or failure of a company. A manipulation of the company’s reported earnings or assets can affect a bank that extends credit to the company, a shareholder who invests money in the company, and those organizations that enter into contracts or agreements with the company.

The manipulation of financial statements also affects employees. It has the power to put employees out of work once the fraud is exposed or collapses. It also has the power to enrich employees – mostly those involved in the fraud, but potentially those who are not. Good financial results (actual or fabricated) can be linked to promotions, raises, enhanced benefit packages, bonuses, and the value of stock option awards.

53.2. Financial statement fraud will cause shareholders to overpay for their investment in the company and they will get less value for their money than they are aware. They may lose part or all of their investment if the company ultimately fails or has to go through some sort of reorganization in order to remain viable. Shareholders also lose the opportunity to invest their money in other companies which may have better actual financial results or which may be more honest in their operations.

53.3. Banks lose money, which affects other bank customers who ultimately make up for those losses and affects the bank’s investors. Creditors can lose large sums of money, which may not have been risked if the creditors knew the true financial condition of the company.

53.4. If enough financial statement frauds occur, or if the frauds are large enough, there are wide-reaching effects for other companies. Consider the case of the Sarbanes-Oxley Act of

2002. The legislation followed the collapse of some large public companies with executives who engaged in significant financial statement fraud.

53.5. This legislation attempted to address financial statement fraud and bring more reliability and transparency to the financial reporting process. Sarbanes-Oxley required companies to make changes, and it also changed how independent auditors do their work.

53.6. The legislation (SOX) has caused companies to collectively spend billions of dollars on assessing their processes, engaging consultants to help with the assessments, and enhanced independent audits. This is an indirect cost of financial statement fraud, but its impact on companies is direct. It has been very expensive.

53.7. Financial statement fraud often doesn't have a readily apparent or direct financial impact on interested parties. But because it is rampant and its indirect costs are so high, it is important that the users of financial statements be aware of the risk and the impact.

53.8. Regulations may be effective in curbing some of this fraud, but a skeptical eye on the part of interested parties might be more effective in protecting investors, creditors, and other business partners from the negative effects of financial statement fraud.

Short Answer Questions on Financial Statement Frauds

Q 1: What does the term "Consideration of Fraud" in a financial statement audit mean?

A: "Consideration of Fraud" in a financial statement audit refers to the specific requirement of conducting an audit with the view that a "misrepresentation on a financial statement could be the result of a fraud". This is also called "professional scepticism". Every auditor is required to assume fraud even when an auditor thinks the management is honest and has never engaged in fraud before.

Q 2: What are some of the indications of a financial statement fraud?

A: Some of the indications of such a fraud includes symptoms such as (a) accounting anomalies, (b) unusual profit or loss, and (c) inappropriate financial actions by management.

Q 3: What are financial statement fraud cases?

A: Financial statement fraud cases are cases where financial statements are manipulated by the corporations, brokerage houses or banks to either encourage investors to invest under false pretences or cheat an account holder out of his money.

Q4: What is financial statement fraud?

A: Financial statement fraud is defined as "misstatement of numbers in financial statement documents". Companies compile financial statements to provide the public and other stakeholders an overview of the revenues and sales. If the figures in the statements are misleading, this would be considered as a financial statement fraud.

Q 5: Which methods are employed for conducting a financial accounting fraud?

A: A financial accounting fraud typically makes use of accounting tricks to depict a financially stronger position by overstating assets, profits and revenues. At the same time, to increase the net worth and equity of the company, losses, liabilities and expenses are understated. Sometimes expenditures are overstated and revenues are understated in order to evade taxes.

Q 6: Can you name some of the warning signs that might indicate the presence of a fraud financial statement for the auditors?

A: Many signals indicate the possibility of a financial statement fraud. Prominent among these are "fragile internal control environment", "management decisions being dominated by an individual or small group", "frequent disputes between senior managers and auditors", and a huge emphasis on earnings and revenue projection. However, these signs only point out the probability that a fraud might be occurring, a significant in-depth analysis in the specific case is required in order to be certain about it.

Q 7: What are the different types of financial statement analysis methods?

A: There are a number of methods used for analysing financial statements. The method chosen usually depends upon the purpose behind the analysis. Some of the most common analysis methods are: external analysis, internal analysis, ratio analysis, horizontal analysis, vertical analysis, and static analysis. Statements are usually analysed to determine the profit or loss, risk factors and overall performance of a firm.

Q 8: Do you think companies that have regular financial fraud investigation checks gain credibility?

A: Financial fraud investigations are important for any organization. Regular checks build the trust of clients or consumers and also keep the employees vigilant. Companies that efficiently manage bribery, frauds and corruption cases are better equipped to handle crisis situations and can analyse the risks and loop holes in the business processes that lead to frauds.

Q 9: Can you tell about the most common types of financial reporting fraud cases?

A: There are seven common occurrences that form the basis of financial reporting fraud cases. These include the following: "fictitious revenues, overstatement of assets, capitalisation of expenses, misappropriation of assets, premature booking of revenues and understatement of expenses and liabilities".

Q 10: How do investigators make financial fraud detection?

A: Financial fraud detection has emerged as a professional field and these experts have the required training to investigate cases of corruption. They look for misappropriation of financial statements, fictitious sales, in-correct asset values, hiding of liabilities, accounting irregularity, weak system of internal control and untraceable deals or third party transactions.

Chapter 19

Opportunities for Chartered Accountants in Forensic Accounting and Fraud Detection

Today's forensic accountants are involved in a wide variety of cases, from the more mundane family law and commercial matters through to a range of criminal investigations, which include white-collar crimes such as business and insurance fraud through to organized crime, murder and even terrorism where forensic accountants are used to trace the money trail and uncover just who is financing the terrorist groups.

Forensic Accounting has taken many great leaps of growth in recent history. The Accounting industry has gradually called for more and more Forensic Accountants. It is predicted that growth of the industry, based on the amount of jobs, will reach 6.7% for the years between 2013 and 2018.

Forensic accounting in India has come to limelight only recently due to rapid increase in Frauds and the white collar crimes and the belief that our law enforcement agencies do not have sufficient expertise or the time needed to uncover frauds. The demand for forensic accountants is exceeding the supply which has given a wide scope to the professionals in this field.

There is no mention of Forensic accountants in the Indian statutes so far but there are various provisions related to Forensic accountants/auditors in the statutes. The introduction of the Companies Act, 2013 has a significant impact on fighting and preventing frauds. Under section 245 (1g) of the new Companies Act, depositors and members of a company can claim damages from auditors, management and other consultants for the wrongdoings by the company and its management. Many consultants and senior executives are expected to become part of the certified community. Further, under section 140 the auditors and their firm would be jointly liable for any frauds in the books of accounts and many auditors are likely to become forensic accountants in the days to come to avoid being caught on the wrong foot. Under section 149(12), independent directors would be held liable for the frauds in their knowledge.

A few of the wide and increasing opportunities of services that Chartered Accountants can best provide are briefly described below:

1. Conventional Investigation assignments as a continuation of audits

These are typical SAP 4 situations where the audit findings have revealed certain anomalies and there is a suspicion of fraud or error. The management may ask the auditors to extend

their audit to apply such extended or modified procedures as may be necessary to assess, evaluate and determine the nature and extent of fraud. This kind of assignment is a regular investigation and needs no elaboration. Such investigations could cover cash embezzlements, asset losses, revenue leakages through inflated or replicated invoices, suppression of income, inflation of liabilities, deflation of receivables and the list could go on and on.

2. Investigations by Statutory authorities

Investigations in respect of violations under any provision under the Income Tax Act, Companies Act, could be required by any of the respective authorities. Even Police, CBI, CID and the Economic Offences wing could need the services of chartered accountants. Such services could include determination of claims from investors of all kinds, assessment of funds lost or misappropriated, non-compliance of prescribed procedures, bank frauds and any other economic offence where knowledge of accounting, record-keeping and relevant applicable laws could be useful. In the recent well published scams such as Harshad Mehta scam, C R Bhansali, Neek Leeson, and Ketan Parikh, large number of chartered accountants have been asked to provide valuable insights as to the nature and methodology of the frauds perpetrated.

3. Bank frauds

This area has the highest potential of fraud. The raw material is money itself. Frauds can be perpetrated within a bank itself or by outsiders. Insiders may manipulate funds, loans, and apply teeming and lading between favored accounts. Outsiders could defraud a bank by furnishing fabricated, duplicated or altered demand drafts, cheques, bills of exchange, and other negotiable instruments. Apart from these borrowers also often cheat banks in hypothecation agreements by inflating inventories or even providing substandard or spurious stocks with little or no value. Chartered Accountants may find themselves as auditors, investigators, or a part of the inspection team. These days even pre facility audits are asked to be carried out. These are audits in the garb of investigations to ensure that funds are going into safe and reliable hands

4. Business risk evaluation.

This is another area of professional opportunity for chartered accountants. Every business venture is always fraught with risks. What varies is the degree and extent of the risk. Take for example a case where a company has to undertake a new project for which it requires a large finance say Rs 100 crores. In the current financial markets there are plenty of consultants offering a plethora of services. Very often such means of financing are obtained through consultants not very well known to the borrowers and possibly of dubious credentials. They offer new and untested financing schemes through banks or financing institutions or IDBI, or RBI, etc. In such situations sometimes upfront or advance payments are to be made which run in substantial amounts. In such circumstances either the financial officers of the company who could be chartered accountants or audit firms may be asked to inquire into the feasibility of the scheme as well as the reliability of the consultant. Since the stakes involved are generally

high, such assignments offer a challenging opportunity for chartered accountants to earn the appreciation of the clients. Similar situations could arise when a new vendor, or a new client or a new venture is to be entered into and the company wants to ensure that there is no risk. In

5. Insurance claim frauds

Claims for loss of stocks and loss of profits of large values, particularly exceeding Rs 5 crores are usually surveyed in detail by most insurance companies. More often than not these claims are inflated, with or without intention. In such situations as well chartered accountants could be called upon to review, inquire and investigate into frauds.

As forensic accountants key assignments like

- Loss Valuers
- Arbitrators
- Empanelment as forensic expert for claims
- And such allied services

6. Compliance verifications

There are so many situations where specific guidelines or directives have been laid down for use of funds. For example a large trust may be given a donation of Rs 10 crores for a project say providing for orphans and widows. The donor may want an assurance that the funds donated have been appropriately used. It is possible that this could turn out to be a thriving ground for frauds and misappropriation of funds. Similarly a hospital may have been given funds for a specific ward with conditions. There could be misrepresentations and false reports. A business may have a remote site where certain activities may be in progress. A possibility of misuse of resources is also likely.

In all such situations, described above, it is not necessary that chartered accountants could be auditors. They could be chief financial officers, treasurers, and accountants, part of the management or even consultants. It is also very essential important to remember that there are no standardized fraud detection methods. Each assignment has to be carried out in a manner appropriate to the Specific needs. The moral is that knowledge dwells within ourselves. Whatever be the impediments in a given situation one can find a solution from an infinite reservoir of knowledge existing within. This analogy cannot be applicable more than in the field of forensics and fraud detection.

7. Fraud Prevention

- Fraud prevention,
- Fraud deterrence
- Fraud detective measures

We as a forensic auditor can provide services at all above three verticals. Eg. Build more stringent internal controls to prevent chances of fraud, implementing strict policy for punishment and zero tolerance attitude [organization would spend even lakhs of rupees to detect, punish and prevent even for a hundred rupee fraud] in the organization for fraud deterrence, to keep some indicators so as to raise red flags, whistle blowers policy as early detective indicators.

In all such situations, described above, it is not necessary that chartered accountants could be auditors. They could be chief financial officers, treasurers, and accountants, part of the management or even consultants. It is also very essential important to remember that there are no standardized fraud detection methods. Each assignment has to be carried out in a manner appropriate to the Specific needs. The moral is that knowledge dwells within ourselves. Whatever be the impediments in a given situation one can find a solution from an infinite reservoir of knowledge existing within. This analogy cannot be applicable more than in the field of forensics and fraud detection.

8. Training

In training available opportunities include

- Conducting Zero fraud tolerance training programs in organizations
- Helping Frame Ethics and Whistle blowing Policies
- Training for basic data analysis to detect indications of fraud
- Collaborating with agencies like CBI, EOW, CAFRAL, NACEN etc. to provide guidance and research on financial forensics
- Working with Universities offering degrees in forensics to develop research material and participating as faculty in areas of financial forensics.
- Developing content and designing courses for regulatory agencies like IRDA, RBI as well as chambers of commerce to create awareness about the Fraud Menace and the capabilities available to combat it
- Partnering with NASSCOM to establish testing and compliance standards for IT firms engaged in software development as well for the outsourcing industry
- Workshops for determining Risk frameworks relevant to particular organizations and industries and Assessment of the extent of exposure after the implementation of Internal Controls
- Specifically tailored courses for members of ICAI focused on the role of auditors in commenting on the adequacy of internal financial controls with reference to their capability to prevent and detect fraud

Chapter 20
Useful Websites

Sr. No.	Name	Website
1	Serious Fraud Investigation Office, India	http://sfio.nic.in/websitenew/main2.asp
2	Serious Fraud Office – UK	http://www.sfo.gov.uk/
3	National Fraud Authority – UK	https://www.gov.uk/government/organisations/national-fraud-authority
4	Action Fraud - UK	http://www.actionfraud.police.uk/
5	UK's Fraud Prevention Service	http://www.cifas.org.uk/
6	Association of Certified Fraud Examiners	http://www.acfe.com/
7	FBI Home page for Fraud	http://www.fbi.gov/scams-safety/fraud/fraud
8	The United States department of Justice – Fraud section	http://www.justice.gov/criminal/fraud/
9	European Anti-Fraud Office	http://ec.europa.eu/anti_fraud/investigations/report-fraud/
10	Canadian Anti-Fraud Centre (CAFC)	http://www.antifraudcentre-centreantifraude.ca/index-eng.htm