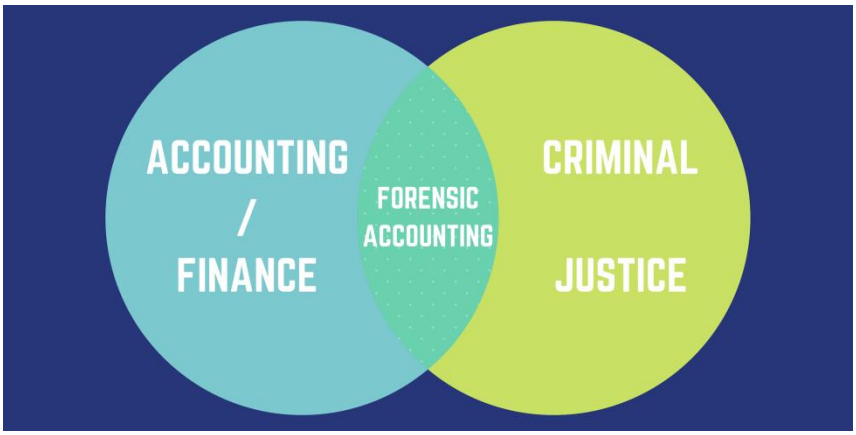
ENCYCLOPEDIA ON FORENSIC INVESTIGATION AND THE ROLE OF FORENSIC ACCOUNTANT



By

CA. (Dr.) Adzuki Rajkumar Satyanarayan

Your Candidate for Central Council Election (ICAI-WIRC) 2021 requesting your FIRST/BEST preference vote to Ballot No. 1 on my credentials and proven record and performance and let us contribute to make India No. 1 economy in world by making contributory services in all levels of economic activities, policy making initiatives through you and ICAI

- **MY MISSION IS TO TRANSFORM CA PROFESSION - MAKE EVERY CITIZEN ECONOMICALLY POWERFUL & INDIA THE MOST POWERFUL NATION OF WORLD !**
- **MY PASSION IS TO MAKE EVERY CA MEMBER & STUDENT SPEAKER & WRITER !**

Author of more than 300 books & Global business, professional growth and motivational coach
Passionate to make anyone Speaker, Writer, Acquiring New Knowledge ,Professional Qualifications , Growth in Business & Promotion As CEO
Member IFAC-PAIB committee 2001-2004; Member IFRS SMEIG London 2018-2020
Ex-director - SBI mutual fund, BOI mutual fund, global mediator and international arbitrator
B. Com (Hons), M.Com, FCA, FCS, FCMA, LL.B, LLM(Constitution),Dip CG, MBA, Dip IFRS (UK), DLL&LW, Dip IPR, Dip in Criminology, Ph. D, Mediation ,IP(IBBI), MBF, Dip HRM, Dip Cyber Law
20+ Certificate courses; 75+ Self Development Courses
Student of : MA(Psychology), MA (Economics), PGD CSR, PGD Crime Investigation
IBBI(RV)++++++++++++++++
Ranks ALL INDIA 1st in Inter CA; 6th in CA Final; 3rd in CMA Final, 5th in Mumbai University +++
Chairman western region ICAI 1997; Council Member ICAI 1998-2016

Mob: 98200 61049; Email: rajkumar@cadrrajkumaradukia.com

By giving your most valuable First/Best Preferential Vote to me,

I vouch you yourself will be the member of the council!

You may read & download my articles from my website:- www.cadrrajkumaradukia.com

PART I

1. What is Forensic Investigation? .....

2. Advantages of Forensic Investigation

3. Evolution of Forensic Investigation in the World .....

4. Evolution of Forensic Investigation in India .....

5. Steps / Conduct of Forensic Investigation – Procedures .....

6. Prevention measures including Internal Finance Control COSO, ERM, COBIT 2019

7. Fraud Risk Assessment.....

8. Forensic Investigation Techniques .....

PART II

9. Forensic Investigation under the Information Technology Act 2000

10. Forensic Investigation under The Insolvency and Bankruptcy Code , 2016

11. Forensic Investigations under the Companies Act 2013

12. Forensic Investigation of Listed corporate entities

PART III

13. Cyber Crime & Security Strategy for Cyber Crime .....

14. Forensic Investigation in Digital Environment .....

15. Common Fraud Techniques in Banking & Insurance Sector .....

16. Common Fraud Techniques in Manufacturing Industry .....

PART IV

17. Role of Forensic Accountants

18. Fraud Prevention and Internal Control Frameworks

PART V

19. Expert Opinion and Report Writing .....

20. Forensic Investigation Report Format .....

21. Formats for Various Undertakings/Certificates.....

22. Useful Websites.....

PART I

1. WHAT IS FORENSIC INVESTIGTION?

The term Forensic Investigation combines the word Forensic which means “scientific tests or techniques used in connection with the detection of crime” and the word Investigation which means “the act or process of examining a crime, problem, statement, etc. carefully, especially to discover the truth”. Combining the two terms, Forensic investigation is the gathering and analysis of all crime-related physical evidence in order to come to a conclusion about a suspect. Investigators will look at blood, fluid, or fingerprints, residue, hard drives, computers, or other technology to establish how a crime took place. Forensic Investigation is carrying out an inquiry conducted in such a manner that the outcome will have application in court of law.

The term Forensic Investigation is very wide and is applied in various disciplines like accounting, medicine and engineering. The scope and type of the investigations is defined by the crime that the investigation intends to investigate. For example if the crime committed is a murder, then Forensic Entomology, Forensic Pathology, Forensic Psychology, Forensic Science, Forensic Toxicology may be used. If the crime committed is fraud or crime related to finance, Forensic Investigation may be conducted and when the crime is conducted through Computers, cyber forensics may be conducted.

Financial Crimes range from tax evasions to theft of company assets to wrong reporting in financial statements. A detail scenario of how frauds are committed was given by Kautilya.

Kautilya, in his famous treatise “Arthashastra” penned down around 300 BC, painted a very graphic detail of what we, in modern times, term as ‘fraud’. Kautilya describes forty ways of embezzlement, some of which are: “what is realized earlier is entered later on; what is realized later is entered earlier; what ought to be realized is not realized; what is hard to realise is shown as realized; what is collected is shown as not collected; what has not been collected is shown as collected; what is collected in part is entered as collected in full; what is collected in full is entered as collected in part; what is collected is of one sort, while what is entered is of another sort.”

Statistics quoted in a recent report by the Association of Certified Fraud Examiners’ (ACFE) 2018 titled “REPORT TO THE NATION ON OCCUPATIONAL FRAUD AND ABUSE”

may have some answers. The report has estimated that in the 2690 cases of fraud reported during the year, the amount of losses were estimated at $7 billion +. 22% of the cases caused losses of more than $1 million. Approximately 30% of the schemes in the study included two or more of the three primary forms of occupational fraud. The smallest organizations tend to suffer disproportionately large losses due to occupational fraud. Additionally, the specific fraud risks faced by small businesses differ from those faced by larger organizations, with certain categories of fraud being much more prominent at small entities than at their larger counterparts. The banking and financial services, government and public administration, and manufacturing industries continue to have the greatest number of cases reported in their research, while the mining, real estate, and oil and gas industries had the largest reported median losses. The higher the perpetrator's level of authority, the greater fraud losses tend to be. Owners/executives only accounted for 19% of all cases, but they caused a median loss of $8,50,000. Employees, conversely, committed 44% of occupational frauds but only caused a median loss of $50,000. Managers ranked in the middle, committing 34% of frauds with a median loss of $150,000. Collusion helps employees evade independent checks and other anti-fraud controls, enabling them to steal larger amounts. The median loss in a fraud committed by a single person was $74,000, but as the number of perpetrators increased, losses rose dramatically. In cases with two perpetrators the median loss was $150,000, for three perpetrators it was $339,000. Approximately 77% of the frauds in the study were committed by individuals working in one of seven departments: accounting, operations, sales, executive/upper management, customer service, purchasing and finance. At the time of our survey, 53% of the victim organizations had not recovered any of their losses due to fraud, and only 15% had made a full recovery. Enron, Worldcom and more recently, the Libor manipulation scandals, have caused major upheavals in western nations and their impact has been felt not only in the individual institutions or countries but across the global financial system. India too has witnessed a spate of fraudulent activities in the corporate sector over the last decade in the form of Satyam, Reebok, Adidas, etc. What the above statistics reveal is that the frequency, volume and the gravity of instances of fraud across various sectors, particularly in the financial sector, has gone up tremendously over the past few years. With the sweeping changes in the scope and magnitude of banking transactions witnessed in the past few decades, the emergence of hybrid financial products, the increasing trend of cross border financial transactions and the dynamics of real-time fund movement and transformation, the vulnerability of the system to the menace of fraud has become higher than ever before.

In criminal law, fraud is intentional deception made for personal gain or to damage another individual. Defrauding people or entities of money or valuables is a common purpose of fraud.

Fraud is defined as ‘a legal concept, which involves acts of deceit, trickery, concealment, or breach of confidence that are used to gain some unfair or dishonest advantage; an unlawful interaction between two entities, where one party intentionally deceives the other through the means of false representation in order to gain illicit, unjust advantage.’ (XVI International Conference of Supreme Audit Institutions (INCOSAI) Uruguay, 1998)

The term ‘forensic’ has usually attracted an unfortunate connotation with the morbid world of forensic medicine. It conjures images of forensic pathologists, battered corpses, and blood - splattered implements at the scenes of crime and autopsies and post mortems. Nothing can be further from the truth. Forensic Investigation shares only one thread in common with forensic pathology. That common denominator is the pursuit of evidence that will stand the rigorous scrutiny that the rules of evidence and procedure demand for its admission as evidence before the courts.

Indeed, the term ‘forensic’ as defined in Webster’s Dictionary means ‘belonging to, used in or suitable to courts of judicature or to public discussion and debate’. The integration of accounting, auditing and investigative skills yields the specialty known as Forensic Investigation. 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*, is a specialized mode of investigation that is suitable to the court which will form the basis of discussion, debate and, ultimately, for dispute resolution whether before the courts or other decision-making tribunals.

Forensic Investigation in its present state can be broadly classified into two categories as under.

1. Encompassing litigation support and
2. Investigative accounting.

These two major categories form the core around which other support services that traditionally come within the sphere of investigative services revolve - including corporate

intelligence and fraud investigation services. However, it would also be remiss not to define what encompasses litigation support and investigative accounting.

1. **Litigation support** - is the provision of assistance of an accounting nature in a matter involving existing or pending litigation. It is primarily focused on issues relating to the quantification of economic damages, which means a typical litigation support assignment would involve calculating the economic loss or damage resulting from a breach of contract. However, it also extends to other areas involving valuations, tracing assets, revenue recovery, accounting reconstruction and financial analysis, to name a few. Litigation support also works closely with lawyers in matters involving, but not limited to, contract disputes, insolvency litigation, insurance claims, royalty audits, shareholders disputes and intellectual property claims.

2. **Investigative accounting** - in contrast, investigative accounting is concerned with investigations of a criminal nature. A typical investigative accounting assignment could be one involving employee fraud, securities fraud, insurance fraud, kickbacks and advance fee frauds. No doubt in many assignments, both litigation support and investigative accounting services are required. In many cases, the combination of these services will not be adequate to address the problem unless there is in place an effective programme for fraud risk management and control. Creating an ethical work environment with a vigorous anti-fraud culture, implemented seriously by senior management through the promotion of a clear anti-fraud policy, is the only viable option if management is serious about preventing or reducing the recurrence of corporate fraud in its various guises.

Emergence of Computer Forensics

The proliferation of e-commerce has led to an increasing e-fraud in recent times, which in turn has meant an increasing demand for forensic IT services aimed at identifying unauthorized or unethical IT activities. It is undeniable that this is the fastest growing forensic discipline that will assume greater importance; hence no paper on Forensic Investigation would be complete without a passing mention of this specialized field.

Computer forensics is simply the application of computer science to the investigative process. As investigative accounting is an important aspect of Forensic Investigation, computer forensics and its sub-disciplines are important tools for the Forensic Investigator in his task of retrieving and analyzing evidence for the purposes of uncovering a fraud or challenging any

financial information critical to the outcome of any dispute. As a full treatment of this area would warrant a separate article, it would suffice to add that the sub-disciplines of computer forensics, like computer media analyses, imagery 0enhancement, video and audio enhancements and database visualization, are tools, techniques and skills which are becoming more critical in the field of Forensic Investigation in general and investigative accounting in particular. Fraud detection services and the techniques of data matching and data mining would be impossible without the application of computer forensics.

Financial Sector Frauds

Bank fraud is the use of potentially illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution. In many instances, bank fraud is a criminal offence. While the specific elements of particular banking fraud laws vary between jurisdictions, the term bank fraud applies to actions that employ a scheme or artifice, as opposed to bank robbery or theft. For this reason, bank fraud is sometimes considered a white-collar crime.

- There are numerous types of financial sector frauds (bank fraud) like stolen cheque, cheque kiting, rogue trader, fraudulent loan and applications for loan, and many more.
- 'Skimming of Card Information takes a number of forms, ranging from merchants copying clients' credit card numbers for use in later illegal activities or criminals using carbon copies from old mechanical card imprint machines to steal the info, to the use of tampered credit or debit card readers to copy the magnetic stripe from a payment card while a hidden camera captures the numbers on the face of the card. Some fraudsters have attached fraudulent card stripe readers to publicly accessible ATMs, to gain unauthorized access to the contents of the magnetic stripe, as well as hidden cameras to illegally record users' authorization codes.
- Phishing operates by sending forged e-mail, impersonating an online bank, auction or payment site; the e-mail directs the user to a forged web site which is designed to look like the login to the legitimate site but which claims that the user must update personal info. The information thus stolen is then used in other frauds, such as theft of identity or online auction fraud.

- Fraudsters may set up companies or create websites with names that sound similar to existing banks, or assume titles conferring notability to themselves for plausibility, then abscond with the deposited funds.

Typical Approach to a Forensic Investigation

There are usually five areas which the forensic investigator will address in his approach towards any case:

1. Focus on the who, what, when, where and how of what happened - this is vital in order to understand the whole situation that is made more complex by the lack of full documentation or other evidence. A thorough analysis and evaluation of what happened would assist in framing the issues for the Forensic Investigator, the management and their lawyers to consider when deciding on what steps to take.
2. Consider all suspects - nobody is ruled out or beyond suspicion.
3. be on the alert for forged documents - seemingly innocuous documents or transactions may hide potential frauds or lead to more incriminating evidence.
4. Conduct extensive searches of company documents and computer files for evidence of fraud - this is where the Forensic Investigator's team of forensic IT personnel would be indispensable in any investigation.
5. Interview key company employees - formally and informally.

Difference between Forensic Investigation and Other Audits

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 investigators and those of financial auditors

Sr. No.	Particulars	Other Audits	Forensic Investigation
1.	Objectives	Express an opinion as to 'True & Fair presentation	Whether any fraud has actually, 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 current assets, provisions / liability estimation, etc.	Relies on the Management certificate / Management Representation	Independent verification of suspected / selected items
5.	Off balance sheet items (like contracts etc.)	Used to vouch the arithmetic accuracy & compliance with procedures.	Regulating& 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 and naming persons behind such frauds.

2. ADVANTAGES OF FORENSIC INVESTIGATION

Forensic Investigation involves examination of legalities by blending the techniques of propriety (Value for Money audit), regularity and investigative and financial audits. The

objective is to find out whether or not true business value has been reflected in the financial statements and in the course of examination to find whether any fraud has taken place.

Why engage a Forensic Investigator?

A logical question to pose is why bring in a forensic investigator and his team when the organization's internal auditor and management team can handle the situation which can range from a simple employee fraud to a more complex situation involving management itself? The answer would be obvious when management itself is involved and the fallout to the discovery of the fraud leads to low employee morale, adverse public opinion and perception of the company's image and organizational disarray generally. Engaging an external party can have distinct advantages from conducting an internal investigation.

Uses of Forensic Investigation:

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

1. **Fraud detection where employees commit Fraud:** Where the employee indulges in fraudulent activities and are caught to have committed fraud, the Forensic Investigator tries to locate any assets created by them out of the funds defalcated, then try interrogating them and trying to find out the hidden truth.
2. **Criminal Investigation:** Matters relating to financial implications the services of the Forensic Investigators are availed of. The report of the accountants is considered in preparing and presentation as evidence.
3. **Cases relating to professional negligence:** Professional negligence cases are taken up by the Forensic Investigators. Non-conformation to Generally Accepted Accounting Standards (GAAS) or noncompliance 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.

4. **Arbitration service:** Forensic investigators render arbitration and mediation services for the business community, since they undergo special training in the area of alternative dispute resolution.

5. **Settlement of insurance claims:** Insurance companies engage Forensic Investigators to have an accurate assessment of claims to be settled.

   Similarly, policyholders seek the help of a forensic investigator when they need to challenge the claim settlement as worked out by the insurance companies. A forensic investigator 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 Investigators to handle contract disputes, construction claims, product liability claims, and infringement of patent and trademarks cases, liability arising from breach of contracts and so on.

7. **Engagement by Regulators:** Regulators of businesses like the Ministry of Corporate Affairs, the SEBI or the stock exchanges engage Forensic Investigators to gather evidence in the cases where they are of an opinion that a fraud or misrepresentation of accounts has been resorted to by the company and detailed investigation in its functioning is necessary for the overall benefit of the stakeholders.

Key Benefits of Using Forensic Investigators

1. **Objectivity and credibility** there is little doubt that an external party would be far more independent and objective than an internal auditor or company accountant who ultimately reports to management on his findings. An established firm of forensic investigators and its team would also have credibility stemming from the firm's reputation, network and track record.

2. **Accounting expertise and industry knowledge** an external forensic investigator would add to the organization's investigation team with breadth and depth of experience and deep industry expertise in handling frauds of the nature encountered by the organisation.

3. **Provision of valuable manpower resources** an organisation in the midst of reorganization and restructuring following a major fraud would hardly have the full-time resources to handle a broad-based exhaustive investigation. The forensic investigator and his team of assistants would provide the much-needed experienced resources, thereby freeing the organization's staff for other more immediate management demands. This is all the more critical when the nature of the fraud calls for management to move quickly to contain the problem and when resources cannot be mobilised in time.

4. **Enhanced effectiveness and efficiency** this arise from the additional dimension and depth which experienced individuals in fraud investigation bring with them to focus on the issues at hand. Such individuals are specialists in rooting out fraud and would recognise transactions normally passed over by the organization's accountants or auditors.

3. EVOLUTION OF FORENSIC INVESTIGATION INVESTIGATION IN THE WORLD

Though Forensic Investigation has gained more publicity in the recent years, evidence shows that it has actually been around for centuries. In fact, archaeological findings reveal that, as far back as 3300-3500 BC, the scribes of ancient Egypt, who were the accountants of their day, were involved in the prevention and detection of fraud.

The name Forensic Investigation wasn't even coined until 1946 implying that this specialty career path was not especially common. Maurice E. Peloubet is credited with developing the term Forensic Accounting in his 1946 essay "Forensic Accounting: Its Place in Today's Economy." By this time, Forensic Accounting had proven its worth during World War II, however formalized procedures were not in place until the 1980's when major academic works were published. The popularity and need for the services Forensic Investigators provide has steadily and more rapidly grown in the past few decades.

In more recent times, a close relationship developed between the accountancy and legal professions in the 1800, with accountants acting as expert financial witnesses in court cases. In 1931, the IRS and FBI used accounting to convict mobster Al Capone. An arrest wasn't made until law enforcement built a tax evasion case utilizing accounting expertise. Frank J. Wilson was the agent charged with finding proof of tax evasion. Wilson sifted through millions of financial documents and found enough evidence for a conviction. Due to the Capone case, the IRS actually produced an ad campaign boasting "Only an Accountant Could Catch Al Capone."

The basis of this field is founded upon understanding the mind of the fraudster in order to understand why frauds are committed. Donald Cressey, a sociologist and criminologist in the 1940s, became a leader in understanding fraudsters and why they do what they do. Cressey wrote, "Theft of the Nation," a treatise on la Cosa Nostra, and he was widely known for his studies in organized crime. Cressey first gained notoriety in this field while completing his PhD dissertation on embezzlers, while at Indiana University. Cressey interviewed nearly 200 incarcerated individuals charged with embezzlement. From his research, Cressey developed "The Fraud Triangle."

So, far from being a new practice, forensic investigation has long been part of the accounting profession. While it took a back seat in the early 20th century with general accounting taking a greater role, it is now merely returning to its traditions.

In 1992, the American College of Forensic Examiners was established. In 1997, the American Board of Forensic Accounts started functioning. In 2000, the Journal of Forensic Accounting, Auditing, Fraud and Taxation began publication. The Sarbanes-Oxley Act established the Public Companies Accounting Oversight Board (PCAOB) in 2002 that was responsible for developing auditing standards, conducting investigations and ensuring corporate compliance. It is because of this act, that Forensic Investigation is gaining importance.

Today's forensic investigators 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 Investigators are used to trace the money trail and uncover just who is financing the terrorist groups.

Sarbanes-Oxley opened up a whole new field of investigation for Forensic Investigators. For one, it requires management to certify that their financial statements are free from material misstatement and fraud. Since the Enron scandal and others like it there has been in increased demand for audits and scrutiny of all companies. Often these audits take a Forensic Investigator with them for their expertise. Forensic Investigators have also been called in to discover whether any misstatements were intentional or by mistake. There is a lot of pressure on management to provide nearly perfect financial statements. Therefore, there is an increase in demand for Forensic Investigators valuable knowledge in that area.

In 2011, the Securities and Exchange Commission issued the Dodd-Frank Act. This piece of legislation is an even bigger motivator for whistle-blowers to come forward. If a whistle-blower brings forward information that results in successful enforcement of monetary penalties over $1,000,000, they will be rewarded monetarily. The award can be from 10-30% of the monetary penalties. This is a huge motivating reason for people to act ethically and bring attention to fraudulent activity within their organization. With that comes more demand for Forensic Investigators to be involved.

Forensic Investigation has taken many great leaps of growth in recent history. The Accounting industry has gradually called for more and more Forensic Investigators. 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.

4. EVOLUTION OF FORENSIC INVESTIGATION INVESTIGATION IN INDIA

In Indian context history of investigative accounting goes back to the ancient Mauryan Times. In India, Kautilya was the first person to mention the famous forty ways of embezzlement in his famous Kautilya Arthashastra.

Forensic Investigation 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. In India the formation of Serious Fraud Investigation Office is the landmark creation for the Forensic Accountants. Growing cyber-crimes, failure of regulators to track the security scams, series 101 of co-

operative banks bursting - all are pinpointing the need of Forensic Investigation, irrespective of whether we understand the need or not.

In India, Forensic Investigation investigation has not got its due recognition even after alarming increase in the complex financial crimes and lack of adequately trained professionals to investigate and report on the complex financial crimes. The Serious Fraud Investigation Office (SFIO) formed by the Government of India under Ministry of Corporate Affairs can be regarded the first step of Government of India to recognize the importance and advance the profession of Forensic Investigators.

There is no mention of Forensic Investigators in the Indian statutes so far but there are various provisions related to Forensic Investigators 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 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 Investigators 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.

5. STEPS / CONDUCT OF FORENSIC INVESTIGATIONS

Fraud is considered to involve misrepresentation with the intent to deceive. If a company makes specific promises about a product, for example, in order to sell that product, they may be guilty of fraud if they are aware that the product does not work as advertised. Fraud is a very real and costly problem in today's world, and it causes not only loss of money but also loss of life and serious injuries. A fraud investigation tries to determine whether fraud has taken place and tries to detect evidence if fraud has occurred.

Just as there are different types of fraud and fraud-related crimes, there are different types of fraud investigations. Insurance fraud investigations, for example, try to uncover those who make false claims to get insurance money. Identity theft investigations try to determine

whether someone's identity has been stolen and used to perpetrate fraud and other type of fraud investigations. General fraud investigations cover all other areas of fraud.

The Forensic investigator's concern is not with reaching a general opinion on financial statements taken as a whole, derived from reasonable efforts within a reasonable materiality boundary. Instead, the forensic investigator's concern is, at a much more granular level, with the detailed development of factual information—derived from both documentary evidence and testimonial evidence—about the who, what, when, where, how, and why of a suspected or known impropriety. Sampling and materiality concepts are generally not used in determining the scope of Forensic Investigation procedures. Instead, all relevant evidence is sought and examined. Based on the investigative findings, the forensic investigator assesses and measures losses or other forms of damage to the organization and recommends and implements corrective actions, often including changes in accounting processes and policies and/or personnel actions. In addition, the forensic investigator takes preventive actions to eliminate recurrence of the problem. The forensic investigator's findings and recommendations may form the basis of testimony in litigation proceedings or criminal actions against the perpetrators.

Broad Stages of Forensic Investigation:

1. Accepting the investigation
2. Planning
3. Evidence Gathering
4. Reporting
5. Court Proceedings

1. Accepting the investigation:

- Forensic Investigators must ensure whether their firm has necessary skills and experience to accept the work.
- Ideally statutory Auditors should not accept forensic investigation assignments of the same concern.

2. Planning or Objectives of the investigation:

- Identify type of fraud
- Identify Fraudsters

• Quantify the loss

• Gather Evidence

• Provide advice to prevent the reoccurrence

3. Gathering Evidence or Technique:

• Testing internal controls

• Use analytical procedures

• Apply CAAT

• Discussion and interviews with employees

• Substantive techniques such as Reconciliation, Cash counts and Review of stocks.

4. Reporting: Report contains

• Findings / observation

• Summary of evidences

• Amount of loss

• How fraudsters set up fraud scheme and which controls were circumvented

• Recommend improvements of control

5. Court Proceedings:

• Members of investigation team are involved

• Evidence gathering is presented

• Simplify technical teams

• Forensic Investigators do not testify that fraud has occurred but only present evidence.

6. Fraud Prevention measures including internal financial control, COSO ERM & COBIT 2019

Fraud and white-collar crime have increased considerably over the last two decades, and professionals believe this trend is likely to continue. The cost to business and the public can only be estimated, as many crimes go unreported. However, the statistics we currently have shown the astronomical values associated with fraud. Also, the expansion of computers into businesses may make organizations more vulnerable to fraud and abuse.

So the question is can frauds be prevented? As the popular saying goes "Prevention is better than Cure". Frauds can definitely be prevented. As the cost that an organization has to pay on account of fraud is generally quite high it is better to put in place techniques that would help the management of the organization to be better equipped to prevent frauds.

How can frauds be prevented?

The Management and Auditor of an organization both have roles to play in the prevention and detection of fraud. Effective Internal control measures are a key to prevent frauds. However they alone are not sufficient. Corporate culture, the attitudes of senior management and all employees, must be such that the company is fraud resistant.

Audit, can take steps to ensure that senior management is aware of the risk and materiality of fraud and that all instances of fraud are made known to all employees.

Effective Internal Controls-

Internal controls are the plans and/or programs implemented to safeguard a company's assets, ensure the integrity of its accounting records, and deter and detect **fraud** and theft. Segregation of duties is an important component of **internal control** that can reduce the risk of **fraud** from occurring.

Internal control Framework- for Fraud Prevention

1. **Use a system of checks and balances to ensure no one person has control over all parts of a financial transaction.**
    - Require purchases, payroll, and disbursements to be authorized by a designated person.
    - Separate handling (receipt and deposit) functions from record keeping functions (recording transactions and reconciling accounts).
    - Separate purchasing functions from payables functions.
    - Ensure that the same person isn't authorized to write and sign a cheque.

- When opening mail, endorse or stamp cheques “For Deposit Only” and list cheques on a log before turning them over to the person responsible for depositing receipts. Periodically reconcile the incoming cheque log against deposits.
- Require supervisors to approve employees’ time sheets before payroll is prepared.
- Require paycheques to be distributed by a person other than the one authorizing or recording payroll transactions or preparing payroll cheques.
- If the agency is so small that you can’t separate duties, require an independent check of work being done, for example, by a board member.
- Require accounting department employees to take vacations.
- For transactions of higher value, make authorization of more than one person mandatory.

2. **Reconcile agency bank accounts every month.**
    - Require the reconciliation to be completed by an independent person who doesn’t have bookkeeping responsibilities or cheque signing responsibilities or require supervisory review of the reconciliation.
    - Examine cancelled cheques to make sure vendors are recognized, expenditures are related to agency business, signatures are by authorized signers, and endorsements are appropriate.
    - Examine bank statements and cancelled cheques to make sure cheques are not issued out of sequence.
    - Initial and date the bank statements or reconciliation report to document that a review and reconciliation was performed and file the bank statements and reconciliations.
3. **Restrict use of agency credit cards and verify all charges made to credit cards or accounts to ensure they were business-related.**
    - Limit the number of agency credit cards and users.
    - Establish a policy that credit cards are for business use only; prohibit use of cards for personal purposes with subsequent reimbursement.
    - Set account limits with credit card companies or vendors.

- Inform employees of appropriate use of the cards and purchases that are not allowed.
- Require employees to submit itemized, original receipts for all purchases.
- Examine credit card statements and corresponding receipts each month, independently, to determine whether charges are appropriate and related to agency business.

4. **Provide Board of Directors oversight of agency operations and management.**
    - Monitor the agency's financial activity on a regular basis, comparing actual to budgeted revenues and expenses.
    - Require an explanation of any significant variations from budgeted amounts.
    - Periodically review the cheque register or general ledger to determine whether payroll taxes are paid promptly.
    - Document approval of financial procedures and policies and major expenditures in the board meeting minutes.
    - Require independent auditors to present and explain the annual financial statements to the Board of Directors and to provide management letters to the Board.
    - Evaluate the Executive Director's performance annually against a written job description.
    - Participate in the hiring/approval to hire consultants including the independent auditors.
5. **Prepare all fiscal policies and procedures in writing and obtain Board of Directors approval. Include policies and/or procedures for the following:**
    - cash disbursements
    - attendance and leave
    - expense and travel reimbursements
    - use of agency assets
    - purchasing guidelines
    - debt collection period and types of incentives to be offered
    - petty cash
    - conflicts of interest
6. **Ensure that agency assets such as vehicles, cell phones, equipment, and other agency resources are used only for official business.**

- Examine expense reports, credit card charges, and telephone bills periodically to determine whether charges are appropriate and related to agency business.
- Maintain vehicle logs, listing the dates, times, mileage or odometer readings, purpose of the trip, and name of the employee using the vehicle. Periodically compare the vehicle logs to the fuel bill to check the consistency of fuel usage average to the trips and distance recorded.
- Periodically review the logs to determine whether usage is appropriate and related to agency business.
- Maintain an equipment list and periodically complete an equipment inventory.

7. **Protect petty cash funds and other cash funds.**
   - Limit access to petty cash funds. Keep funds in a locked box or drawer and restrict the number of employees who have access to the key.
   - Require receipts for all petty cash disbursements with the date, amount received, purpose or use for the funds, and name of the employee receiving the funds listed on the receipt.
   - Reconcile the petty cash fund before replenishing it.
   - Limit the petty cash replenishment amount to a total that will require replenishment at least monthly.
   - Verify the petty cash with the balance as per the ledger at the start and close of each day.
   - Keep patient funds separate from petty cash funds.
8. **Protect cheques against fraudulent use.**
   - Prohibit writing cheques payable to cash.
   - Deface and retain voided cheques.
   - Store blank cheques in a locked drawer or cabinet, and limit access to the cheques.
   - Require that cheques are to be signed only when all required information is entered on them and the documents to support them (invoices, approval) are attached.
   - Require two signatures on cheques above a specified limit. Require board member signature for the second signature above a higher specified limit. (Ensure that blank cheques are not pre-signed.)
   - Mark invoices “Paid” with the cheque number when cheques are issued.
   - Enable hidden flags or audit trails on accounting software.

9. **Protect cash and cheque collections.**
    - Ensure that all cash and cheques received are promptly recorded and deposited in the form originally received.
    - Issue receipts for cash, using a pre-numbered receipt book.
    - Conduct unannounced cash counts.
    - Reconcile cash receipts daily with appropriate documentation (cash reports, receipt books, mail tabulations, etc.)
    - Centralize cash receipts whenever possible.
10. **Avoid or discourage related party transactions.**
    - Require that a written conflict of interest and code of ethics policy is in place and that it is updated annually.
    - Require that related party transactions be disclosed and be approved by the Board.
    - Require competitive bidding for major purchases and contracts.
    - Discourage the hiring of relatives and business transactions with Board members and employees.
    - In case, where related party transaction has to be entered into, make a policy to conduct adequate market research to decide the arm's length price for the transaction. Document the research along with the documents/contracts of the related party transaction.

There is little doubt that digitalization is changing almost every business process in every industry. It is already making a huge difference to established leaders in the hospitality, banking, and transportation sectors. It is also helping market entrants with new business models rapidly gain market share. Even traditional sectors such as automotive and utilities, historically protected by heavy asset investments, are beginning to see major disruptions to their business models and their positions in the market. With digitization there is a very strong need for having proper systems in place that would help in preventing and detecting frauds in a cyber environment.

Depending on the level of the assessed risk, IT auditors may choose to increase the depth of testing in areas that are deemed especially susceptible to fraud In reviewing the nature of access to key assets, one cannot help but return to the basics of IT audit. Who holds the keys (privileged users, temps, contractors or business partners), where the keys are located

(unknown backdoor accounts), when the keys are changed (password changes), what keys are available to an individual at any given time (pervasive access across systems) and how the keys are used (collusion either with another insider or an external party) are some of the questions that need to be tackled. In a highly outsourced IT environment, IT auditors may choose to prioritize the testing of third-party controls such as account provisioning and service-level monitoring. In a smaller company environment in which root access to key systems is held by one or selected administrative users, more attention may be required of generic system accounts and frequency of password changes. In a larger organization, a single sign-on solution may come under scrutiny for its potential to unlock excessive system access with a single unauthorized account.

A robust business process possesses the requisite checks and balances (or segregation of duties) that precludes any one individual from taking a transaction from start to finish without an additional pair of eyes. In assessing risks associated with transaction processing, auditors invariably perform an end-to-end review of key classes of transactions, examining the mix of upstream vs. downstream, automated vs. manual controls that impact accuracy, completeness and validity. Opportunities for fraud arise in part from the absence of these business controls.

The COSO Internal Control – Integrated Framework

The COSO *Internal Control – Integrated Framework*[4] has become the generally accepted standard for designing and implementing systems of internal control and assessing the effectiveness of internal control.[5]

While the COSO *Framework* was updated in 2013, its definition of internal control and the components of internal control have remained unchanged from the original framework:

Definition of internal control:

- Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

Components of internal control:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring activities

Internal control is not unidimensional. A deficiency or a change in one of the components can have repercussions throughout all the components, which should be appropriately addressed by management. For example, risk assessment not only influences the control environment and control activities but also may highlight a need to reconsider the entity's requirements for information and communication or for its monitoring activities.

Addressing Fraud with a Strong Control Environment

In establishing a control environment, management must consider the potential for fraud in assessing risks to the achievement of an entity's objectives and be knowledgeable about the various ways that fraud can occur. As part of the process for identifying and analyzing fraud risks, management forms a basis for determining how such risks should be managed and establishes controlandmonitoring activities, formalized in policies and procedures, to help ensure that management directives to mitigate fraud risks to the achievement of objectives are communicated and carried out.

While no control activity can stop a person who is determined to commit a fraud from doing so, a strong control environment, combined with an understanding of the incentives to commit fraud, acts as a form of preventive control against fraud by making the potential perpetrator assess the high risk of getting caught. Conversely, a weak control environment provides opportunity to those thinking of committing a fraudulent act because the risk of getting caught is low.

In this regard, a variety of transaction control activities can be selected and developed to address fraud risk, which in its basic form includes such actions as authorizations and approvals, verifications, reconciliations, and restrictions (physical controls and technology access controls). Segregation of duties and job rotation are typically built into the selection and development of such control activities. Additionally, variance analysis can be used to manage operations and identify possible areas of fraud by directing attention to areas that appear unusual; the preventive control being the establishment of

budgeting and standard cost accounting systems that compare actual results to budgets or standards and the detective control being management follow-up in investigating the reasons for a variance from the budget or standard, which may be indicative of fraud, or at the very least require a management response to correct an apparent operational problem.

Pre-Emptive Fraud Auditing

The primary factor that distinguishes fraud from error is whether the underlying action is intentional or unintentional. Moreover, attempts are made to conceal fraud. This makes looking for fraud a lot like looking for the proverbial needle in a haystack, or as a recent U.S. Secretary of Defence put it, "We don't know [what] we don't know."

EisnerAmper's pre-emptive fraud auditing approach addresses the "unknown unknowns" by proactively anticipating scenarios where fraud may occur and designing monitoring activities, using data-mining techniques combined with statistical and other quantitative analysis, to identify possible instances of fraud.

Data Mining and Statistical Analysis

Business transactions generate data to accomplish the primary purpose for which it was collected; for example, the preparation of financial statements and various types of management reports. When this primary data is accumulated entity-wide, however, it becomes a stand-alone island of unrelated information, or secondary data.

The objective of data mining is to take disparate data and convert it into relevant information, transforming an organization from an accumulator of unrelated data into a proactive responder to risk.

Data-mining techniques can be developed to look for patterns and trends not evident in large amounts of secondary data, looking for the unknown unknowns in an attempt to draw inferences from such patterns and trends. For example, a database may include data that does not conform to the general rule derived for the data set or the general behaviour of other data elements.[11]

No single professional discipline possesses the knowledge and expertise needed to identify data anomalies that require further investigation. A combination of experts – such as information-technology professionals, corporate and compliance attorneys, subject matter and industry experts, internal and external accountants and auditors, Forensic

Investigators, and financial analysts – and those with quantitative data analysis and correlation skills, such as statisticians, are needed.

Data anomalies are referred to as outliers, and while outliers are usually discounted when making a statistical inference regarding a population taken from a sample, outliers should be examined closely when looking for the unknown unknowns in secondary data. Outliers can be identified by measuring the way data are dispersed around the mean.

Points of Focus COSO Principle 8

An organization must consider the potential for fraud when assessing risks to the achievement of objectives.

First, consider the various ways that fraud and misconduct can occur.

1. **Fraudulent reporting:** When an entity's reports, financial and nonfinancial, do not achieve financial reporting objectives because such reports are wilfully prepared with omissions or misstatements.
    1. **Fraudulent financial reporting:** An intentional act designed to deceive users of external financial reports that may result in a material omission from or misstatement of such financial reports.
        1. Includes **misappropriation of assets** where the effect may cause a material omission or misstatement in the external financial reports.
    2. **Fraudulent nonfinancial reporting:** An intentional act designed to deceive users of nonfinancial reporting – including sustainability reporting, health and safety, or employment activity – that may result in reporting with less than the intended level of precision.
    3. **Illegal acts:** Violations of laws or governmental regulations that could have a direct or indirect material impact on the external financial reports.
2. **Loss of assets:** Protecting and safeguarding assets against unauthorized and wilful acquisition, use or disposal, including
    1. Theft of assets
    2. Theft of intellectual property
    3. Illegal marketing
    4. Late trading
    5. Money laundering

6. Other related risks:
    1. Waste
    2. Abuse
    3. Neglect

3. **Corruption:**
    1. By entity personnel
    2. By outsourced service providers directly impacting the entity's ability to achieve its objectives
4. **Management override:** Acts taken by management to override an entity's controls for an illegitimate purpose including personal gain or an enhanced presentation of an entity's financial condition or compliance status.

Second, assess incentives and pressures, opportunities, and attitudes and rationalizations. Work incentives may not be aligned with business goals and objectives that, by their nature, create pressures within the organization. Or there are excessive pressures put on employees to achieve unrealistic performance targets, particularly in the short-term, which may be coupled with a weak control environment that creates opportunities for fraudulent behaviour, along with attitudes and rationalizations that claim to justify such actions.

Changes to the COSO ERM Framework

The seemingly simple act of changing the title of the COSO framework from 2004's "Enterprise Risk Management—Integrated Framework" to the new "Enterprise Risk Management—Integrating with Strategy and Performance" represents a significant shift in approach. COSO recognizes the "dynamic, integrated nature of ERM that begins with the mission, vision and core values of the organization through to the creation of enhanced value."

The updated COSO Enterprise Risk Management Framework is described as:

- More clearly connecting enterprise risk management with a range of stakeholder expectations;
- Positioning risk in the context of an organization's performance, rather than as the subject of an isolated exercise;

- Enabling organizations to better anticipate risk so they can get ahead of it, with an understanding that change creates opportunities, not simply the potential for crisis;
- Emphasizing how ERM informs strategy and performance.

Since the 2017 version of the COSO ERM framework was a dramatic shift from the 2004 version, direct comparisons are difficult to make. That said, there are a number of specific differences worth noting:

1. The updated version states that the purpose of effective enterprise risk management is to help boards and management optimize outcomes to best create, preserve and ultimately realize value.
2. COSO's definition of "risk" changed to reflect its evolved viewpoint that the focus of enterprise risk management is no longer principally on preventing the erosion of value and minimizing risk to an acceptable level. In the 2004 version, the definition read, "Risk is the possibility that an event will occur and *adversely* affect the achievement of objectives" [emphasis added]. The 2017 version reads, "Risk is the possibility that events will occur and affect the achievement of objectives."
3. Rather than simply viewing risk management as an extension of COSO's Internal Controls Framework (the basis for the 2004 version) with a primary focus on the environment within an organization, the updated version explores enterprise risk management by evaluating a particular strategy, considering the possibility that strategy and business objectives may be misaligned, and looking at the risk to implementing the strategy and business objectives.
4. The 2004 version focused on how the risk management process (objective-setting, identification, assessment, control activities, information, communication and monitoring) was implemented at each level of an organization (entity, division, business unit and subsidiary). The 2017 version, on the other hand, consists of five interrelated components of ERM. Three are related to common organizational processes (strategy and objective-setting; performance; and review and revision) and two are supporting factors (governance, culture and information; communication and reporting). Within these five components are 20 principles that represent the fundamental activities that organizations should engage in as part of their ERM practices.
5. As with the ISO update, the COSO revision discusses the important influences that culture and biases carry in decision-making and risk management practices.

6. The revision includes appendices that outline common roles and responsibilities for ERM (such as modifying "lines of defence" to "lines of accountability") and provides illustrations as a guide for developing risk profiles.

What is COBIT

COBIT stands for Control Objectives for Information and Related Technology. It is a framework created by the ISACA (Information Systems Audit and Control Association) for IT governance and management. It was designed to be a supportive tool for managers—and allows bridging the crucial gap between technical issues, business risks, and control requirements. COBIT is a thoroughly recognized guideline that can be applied to any organization in any industry. Overall, COBIT ensures quality, control, and reliability of information systems in organization, which is also the most important aspect of every modern business.

Today, COBIT is used globally by all IT business process managers to equip them with a model to deliver value to the organization and practice better risk management practices associated with the IT processes. The COBIT control model guarantees the integrity of the information system.

COBIT 2019

With a focus on risk, COBIT 2019 worked across many of the most used standards to create a universal "best practices" for building controls. ISACA recognized the way businesses increasingly incorporate vendors into their data ecosystems. As such, they aligned COBIT 5 to ITIL, ISO 2000 and 27000 series, and Project Management Institute (PMI) frameworks to ease the burden of working with multiple standards.

With COBIT 2019, you're focusing on both IT and enterprise level risks. At its core, COBIT 2019 updates COBIT 5 to make it more flexible and focus on individual, organizational needs.

What is new to COBIT 2019?

While COBIT 5 focused on five core principles that appeared to be distinct from one another, COBIT 2019 looks at the way these principles integrate. Each component, now called "Core

Processes," incorporate how to set up the controls as well as the different governance needs. Thus, rather than having two separate sections that users need to integrate on their own, COBIT 2019 focuses on providing a list that starts with objectives and then drills down to how to set those up within the IT environment *as well as* how to align them to skill and culture within your company.

Terminology Changes

COBIT 2019 changes several terms while keeping the fundamental principles in place. "Enablers" are now "Components of the Governance System." "IT Related Goals" are now called "Alignment Goals." "Process Guidance" is changed to "Governance/Management Objectives" to reinforce the integration of the various components.

New Management Objectives

COBIT 2019 added APO14- Managed Data, BAI11 – Managed Projects, and MEA04 – Managed Assurance

Integration of governance and management

1. COBIT 2019 establishes a "goals cascade" that starts with stakeholder drivers and needs and ends with governance and management objectives.
2. Objectives increased from 37 to 40
3. Changes the term "enablers" to "components."
4. Clearly relates components to both governance and management

Additional guidance for governance components

By promoting integration between governance and management, the alignments for processes now incorporate guidance for each governance component which focuses on establishing "capability levels" for each activity.

Four Focus Areas

Cobit 5 created “enabling” processes. COBIT 2019 changes these to create four focus areas: DevOps, Small and Medium Enterprises, Risk, Information Security.

Increased communication

To effectively govern an IT program, you need to know how information flows across the enterprise. COBIT 2019 enables this by providing you with a clear list of what needs to be done and how that needs to be communicated using the terms “input” and “output.”

Tailored Agile Approach

COBIT 2019 recognizes organizations’ continuous monitoring needs. Thus, it created a new process for ongoing improvements. While governance continues to ask business operations and enablement questions, management must not only design and execute plans but review effectiveness to determine benefits. As part of this, change enablement takes on a stronger role, incorporating a continuous improvement cycle.

A COBIT 2019 Audit Checklist

Board Governance

- Define stakeholder (internal and external)
- Define stakeholder needs
    - Create a defined organizational structure
        - Ensure appropriate responsibility and accountability listed within the structure
    - Review people, skills, and competencies
        - Update access and authorization based on role, skills, and need
- Define enterprise goals
    - Create a code of culture, ethics, and behaviour
- Define alignment goals for management of IT
    - Establish a list of processes
    - Determine lines of communication between internal and external stakeholder
- Establish governance and management objectives
    - Set principles, policies, and procedures for management to follow
    - Engage in risk analysis over services, infrastructure, and applications

Senior Management

- Determine drivers
    - Initiate program
    - Define internal controls
- Review the current risk profile and controls
    - Establish an implementation team across enterprise stakeholders
    - Determine effective controls
    - Review weak controls
- Determine future
    - Identify key stakeholders and define roles
    - Determine vendor service levels and create service level agreements that define controls
    - Communicate outcome
- Determine next steps
    - Plan program
    - Execute plan
    - Operate and use
- Review performance
    - Establish key performance indicators
    - Review performance and adjust accordingly

IT Department

- Continuously monitor control effectiveness
    - Recognize the need for changes
- Assess current and changing risks to IT environment
- Define controls
- Build improvements
- Implement improvements
- Measure control effectiveness
- Evaluate IT security risk based on monitoring

IFC-Internal Financial Controls

- As enumerated under Sec 134(5) of Companies Act, 2013("Act"), the Directors Responsibility Statement shall include a declaration from Director that internal financial controls to be followed by the company and that such internal financial controls are adequate and were operating effectively.

- Thus as stated in the explanation under the said section: IFC "means the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information"

Why IFC?

- Since the Act, envisages significant changes in the provisions related to governance, e-management, compliance and enforcement, disclosure norms, auditors and mergers. The Internal Control will enhance the applicability of provisions of the Act. It would give more power in the hands of shareholders and the Government.

- IFC gained its importance after Satyam imbroglio which erupted in 2009. Internal financial controls are designed to provide reasonable assurance that a company's financial statements are reliable and prepared in accordance with the law.

Provisions under Act for IFC

1. Section 134 of the Act

   In case of Listed Companies the Directors responsibility statement states that IFC shall be followed by the company and all the IFC are adequate and were operating effectively.

2. Section 143 of the Act

   Pursuant to Sec 143(3) (i) has stated that the Auditors report shall state whether the company has adequate IFC system in place and the operating effectiveness of such controls

3. Section 177 of the Act

   As per Sec 177(5) the Audit Committee shall call for the Comments of the Auditors about Internal Control system before submission to the Board.

   Pursuant to Sec 177(4) (vii), the Audit Committee shall act in accordance with the terms of reference specified in writing by the Board pertaining to evaluation of IFC

4. Section 149(8) of the Act

   Section 149(8) states the company and Independent Directors have to abide by Schedule IV. The said schedule has put the onus on Independent Directors to satisfy them that the financial control and risk management are robust and defensible.

New Provisions in the Act for Internal Control

5. Inclusive definition of KMP (Key Management Personnel) has made them liable in the event of default. As defined in Sec 2(51) of the Act, KMP would include the Chief Executive Officer or the managing director or the manager; the company secretary; the whole-time director; the Chief Financial Officer; and such other officer as may be prescribed. In case of Sec 2(60) of the Act the Officer in Default includes KMP thus the onus on KMP has increased to maintain the compliance of Internal Controls.

6. Precisely defining Independent Director under Sec 2(47) of the Act, setting up criteria under Sec 149(6) for appointment of Independent Director and a specific composition of Board has enhanced the involvement of all Directors has envisaged prompt and transparent decision making.

7. According to Sec 245 of the Act, Class Action Suits can be filed against Company, Directors, Audit Firms, Expert, Advisor, Consultant or any other person and appointment of small shareholder director has enhanced the participation and accountability of stakeholders.

Whistle Blower Policy under Sec 177(9)

8. Setting up of NCLT/NCLAT a specialized quasi-judicial body to faster and prompt resolution of corporate issues.

Disclosures

1. Directors Responsibility Statement
2. Maintenance of Electronic Records
3. Disclosure as per Clause 55 of Listing Agreement
4. Tenure of Auditors and not refrain then for rendering certain services
5. Secretarial Audit as per Sec 204 of the Act

.

7. FRAUD RISK ASSESSMENT

What is Fraud Risk Assessment?

Fraud risk assessment is the evaluation of potential instances of fraud that could impact the organization's ethics and compliance standards, business practice requirements, financial reporting integrity, and other objectives. This is typically performed as part of a broader organization-wide risk assessment, and involves subject matter experts from key business functions where fraud could occur (e.g., procurement, accounting, and sales) as well as forensic specialists e.g. Certified Fraud Examiners (CFEs).

The foundation of an effective fraud risk management program should be seen as a component of a larger enterprise risk management (ERM) effort and is rooted in a risk assessment that identifies where fraud may occur and who the perpetrators might be Involves asking questions such as:

1. How might a fraud perpetrator exploit weaknesses in the system of controls?

2. How could a perpetrator override or circumvent controls?
3. What could a perpetrator do to conceal the fraud?
4. What has happened in the past?
5. Can we prevent it?
6. Can we catch it right away?
7. Can we handle it?

Involves asking questions such as, where is fraud inherently high:

- By functional area
- By position
- By Relationship

A fraud risk assessment is a critical tool for managing the cost of fraud to an organization. In its simplest form, the risk assessment is a listing of possible fraud risks to an organization. In its more advanced form, the document not only assesses the likelihood of fraud's occurring within an organization, but becomes an impact statement as well.

From an audit perspective, the fraud risk assessment is the initiation point for the fraud audit program, as its substance is critical in the building of such a program. This substance should include the following:

- A comprehensive listing of all fraud risks facing an organization.
- A likelihood assessment of the fraud risk occurring.
- An understanding of the resulting impact.

Purpose of Risk Assessment

Risk assessment is intended to provide management with a view of events that could impact the achievement of objectives. It is best integrated into existing management processes and should be conducted using a top-down approach that is complemented by a bottom-up assessment process. Boards of directors—and particularly board audit committees—often request enterprise-wide risk assessments to ensure that key risks are identified and duly addressed. Such risk assessments should not be disconnected from other assessments

performed within the organization. The internal audit function, for instance, may be assessing risks to plan its audits for the year. The finance function may look at similar information to perform its risk-based scoping. Business units may also be assessing risks from a business planning or performance management perspective. These individual assessments should be aligned (e.g., using common terminology, risk categories, and congruent outcomes), to cover key objectives, and be integrated to contribute to an enterprise-wide risk assessment.

Types of Risk Assessments

- **Strategic risk assessment**. Evaluation of risks relating to the organization's mission and strategic objectives, typically performed by senior management teams in strategic planning meetings, with varying degrees of formality.
- **Operational risk assessment.** Evaluation of the risk of loss (including risks to financial performance and condition) resulting from inadequate or failed internal processes, people, and systems, or from external events.
- **Compliance risk assessment.** Evaluation of risk factors relative to the organization's compliance obligations, considering laws and regulations, policies and procedures, ethics and business conduct standards, and contracts, as well as strategic voluntary standards and best practices to which the organization has committed. This assessment is typically performed by the compliance function with input from business areas.
- **Financial statement risk assessment.** Evaluation of risks related to a material misstatement of the organization's financial statements through input from various parties such as the controller, internal audit, and operations.
- **Internal audit risk assessment.** Evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives. This top-down approach enables the coverage of internal audit activities to be driven by issues that directly impact shareholder and customer value, with clear and explicit linkage to strategic drivers for the organization.
- **Market risk assessment.** Evaluation of market movements that could affect the organization's performance or risk exposure, considering interest rate risk, currency risk, option risk, and commodity risk. This is performed by market risk specialists.
- **Credit risk assessment.** Evaluation of the potential that a borrower or counterparty will fail to meet its obligations in accordance with agreed terms. This considers credit risk

inherent to the entire portfolio as well as the risk in individual credits or transactions. Conducted typically by credit analysts

- **Customer risk assessment.** Evaluation of the risk profile of customers that could potentially impact the organization's reputation and financial position. This assessment weighs the customer's intent, creditworthiness, affiliations, and other relevant factors. This is typically performed by account managers, using a common set of criteria and a central repository for the assessment data.
- **Product risk assessment.** Evaluation of the risk factors associated with an organization's product, from design and development through manufacturing, distribution, use, and disposal. This assessment aims to understand not only the revenue or cost impact, but also the impact on the brand, interrelationships with other products, dependency on third parties, and other relevant factors. This type of assessment is typically performed by product management groups.
- **Security risk assessment.** Evaluation of potential breaches in an organization's physical assets and information protection and security. This considers infrastructure, applications, operations, and people, and is typically performed by an organization's information security function.
- **Information technology risk assessment.** Evaluation of potential for technology system failures and the organization's return on information technology investments. This assessment would consider such factors as processing capacity, access control, data protection, and cybercrime. This is typically performed by an organization's information technology risk and governance specialists.
- **Project risk assessment.** Evaluation of the risk factors associated with the delivery or implementation of a project, considering stakeholders, dependencies, timelines, cost, and other key considerations. This is typically performed by project management teams.

Fraud Risk Assessment

- Process of Identifying and Analyzing Risks (Sample Fraud Risk Assessment tool)
- Brief background of what constitutes fraud
- Share Resources tools to utilize in fraud risk management
- Common challenges in Effective Fraud Risk Assessment

Importance of Fraud Risk Assessment

- Effective risk assessment is increasingly important to the success of any business
- Relationship of Fraud Risk assessment with enterprise risk management program
- Training received is a very good basis for implementing an anti-fraud programme. A trained leader/staff/Entrepreneur is an important asset
- The environment and business world we operate requires responsible persons in positions of authority to lead the way with knowledge on fraud and set the tone at the top.

Preparing a Fraud Risk Assessment

The fraud risk assessment can be thought of as a fraud deterrence control for organizations in their managing the cost of fraud. It is also the document auditors rely upon to plan their response to the risk of fraud. The preparer of the fraud risk assessment should strive for the following attributes:

- The determination of the fraud likelihood assessment should be free from bias.
- Provides a consistent qualitative and quantitative calculation for assessing the fraud likelihood and the exposure identification.
- Ensures a complete identification of fraud risk based on the primary fraud classifications.

The initial assessment of fraud risk should consider the inherent risk of particular frauds occurring in the absence of internal controls. After all relevant fraud risks have been identified; internal controls are mapped to the identified risks. Fraud risks that remain unaddressed by appropriate controls comprise the population of residual fraud risks.

1. **Identify inherent fraud risk** — Gather information to obtain the population of fraud risks that could apply to the organization. Included in this process is the explicit consideration of all types of fraud schemes and scenarios; incentives, pressures, and opportunities to commit fraud; and IT fraud risks specific to the organization.
2. **Assess likelihood and significance of inherent fraud risk** — assess the relative likelihood and potential significance of identified fraud risks based on historical information, known fraud schemes, and interviews with staff, including business process owners.

3. **Respond to reasonably likely and significant inherent and residual fraud risks** — decide what the response should be to address the identified risks and perform a cost-benefit analysis of fraud risks over which the organization wants to implement controls or specific fraud detection procedures.

10. FINDING RED FLAGS

A red flag is a set of circumstances that are unusual in nature or vary from the normal activity.

It is a signal that something is out of the ordinary and may need to be investigated further.

The first step in fraud detection is, knowing where to look. Understanding the motivations of those committing fraud and knowing in which accounts fraud is more likely to exist based on a risk assessment helps identify the areas that might be subject to greatest scrutiny. Similarly, being aware of the types of transactions that warrant further review, as well as other potential red flag indicators, may alert auditors to areas that might require a closer look.

An auditor's ability to detect fraud may be significantly enhanced by personal understanding of an enterprise and the environment in which it operates. With this knowledge, the auditor may be better able to identify anomalies or other potential red flags such as nonsensical analytic relationships, control weaknesses, transactions that have no apparent business purpose, related parties, and unexpected financial performance. It is important to understand the business, the control procedures in place, the budgeting process, the accounting policies, the industry, and the general economic climate affecting the company.

It is however not as easy as it sounds to identify and interpret potential red flags. The term flags are a bit of a misnomer and creates a false impression of plainly visible warning signs. While this is true in case of some frauds, one should remember that fraud is fundamentally a crime of deception and deceit. Calling to mind a mental picture of a scarcely visible red thread waving in the wind is more accurate than picturing a bold red flag.

The Fraud Triangle

Donald Cressey, a sociologist and criminologist in the 1940s, became a leader in understanding fraudsters and why they do what they do. Cressey wrote, “Theft of the Nation,” a treatise on la Cosa Nostra, and he was widely known for his studies in organized crime. Cressey first gained notoriety in this field while completing his PhD dissertation on embezzlers, while at Indiana University. Cressey interviewed nearly 200 incarcerated individuals charged with embezzlement. From his research, Cressey developed “The Fraud Triangle.”

The fraud triangle views the following as key conditions that tend to be present when fraud occurs:

- Incentive and pressure—that is, need
- Opportunity
- Rationalization and attitude

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 p art 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. These risk factors include:

- Circumstances that threaten the profitability or financial stability of the business
- Excessive pressure on management to meet or exceed the expectations of third parties, including investors and lenders

- Significant threats to the personal wealth of management as a result of the performance of the business
- Excessive internal pressures on divisional or departmental management imposed by the board of directors or senior management
- A struggle to retain the company's listing on a stock exchange or debt rating
- Inability to meet debt covenants or satisfy conditions in merger or acquisition agreements

Opportunity

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.

Risk factors indicative of opportunities that could lead to material misstatements as a result of fraudulent financial reporting include:

- Factors related to the nature of the industry in which the entity operates, the nature of the entity's business and the transactions it enters into, and the manner in which they are recorded in the profit-and-loss account or balance sheet.
- The nature of the entity's relationships with customers and suppliers and its position in its markets: the ability to dominate or dictate terms may create the opportunity for inappropriate or non-arm's-length transactions.
- The degree of judgment involved in determining the level of income or expenditure or the valuation of assets or liabilities: Generally, a higher degree of judgment will give rise to a greater opportunity for deliberate manipulation.

- The extent and effectiveness of supervision of senior management by independent corporate governance functions such as the audit committee, nonexecutive directors, and supervisory boards.
- The degree of complexity and stability of the entity or group.
- The overall control environment, including the continuity and effectiveness of internal audit, information technology, and accounting personnel as well as the effectiveness of accounting and reporting systems.

Rationalization and attitude

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. Risk factors to look for, in this somewhat intangible but critically important category, include:

- Lack of clarity or communication about corporate ethical values or infrequent communication and reinforcement of such values
- Disregard for the risk of fraud—or ineffective measures when fraud rises
- Lack of realism in budgeting and forecasting and in communicating expectations to third parties
- Recurring attempts by management to justify inappropriate accounting or disclosure policies and practices on grounds of materiality or other grounds
- Difficult relationships with the entity's auditors: a bullying attitude, imposition of unreasonable time pressure, or constraints on access to relevant audit evidence

PART II

11. LAWS GOVERNING FRAUDS & INSTITUTIONAL FRAMEWORK IN INDIA AND WORLDWIDE

LAWS GOVERNING FRAUDS IN INDIA

1. The 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. The code was drafted in 1860 on the recommendations of first law commission of India established in 1834 under the Charter Act of 1833 under the Chairmanship of Thomas Babington Macaulay. It came into force in British India during the early British Raj period in 1862. However, it did not apply automatically in the Princely states, which had their own courts and legal systems until the 1940s. The Code has since been amended several times and is now supplemented by other criminal provisions. Based on IPC, Jammu and Kashmir has enacted a separate code known as Ranbir Penal Code (RPC).

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

2. The 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.

To give uniformity to Civil Procedure Legislative Council of India, enacted Code of Civil Procedure, 1859, which received the assent of Governor-General on 23 March 1859. The Code however, not applicable to Supreme Court in the Presidency Towns and to the Presidency Small Cause Courts. But it did not meet the challenges and was replaced by Code

of Civil Procedure Code, 1877. But still it did not fulfil the requirements of time and large amendments were introduced. In 1882, it were recast the whole Code and it was the Code of Civil Procedure, 1882. With passing of time it is felt that the Code needs some flexibility to breathe the air of speed and effectiveness. So, meet these problems Code of Civil Procedure, 1908 was enacted. Though it has been amended number of time it stood the test of time.

The CPC is composed of two parts:

- **First part:** Dividend into 158 Sections. Can be amended by the legislature only.
- **Second Part:** Divided into 51 Orders and Rules. Can be amended by High Courts.

The Orders and Rules are to be read along with the Sections. When there is ambiguity in interpretation between the two, the version of the Sections prevails.

3. The 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."

4. The 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.

The enactment and adoption of the Indian Evidence Act was a path-breaking judicial measure introduced in India, which changed the entire system of concepts pertaining to admissibility of evidences in the Indian courts of law. Until then, the rules of evidences were based on the traditional legal systems of different social groups and communities of India and were different for different people depending on caste, religious faith and social position. The Indian Evidence Act and introduced a standard set of law applicable to all Indians.

Contents of the Act

This Act is divided into three parts and there are 11 chapters in total under this Act.

Part 1 deals with relevancy of the facts. There are two chapters under this part: the first chapter is a preliminary chapter which introduces to the Evidence Act and the second chapter specifically deals with the relevancy of the facts.

Part 2 consists of chapters from 3 to 6. Chapter 3 deals with facts which need not be proved, chapter 4 deals with oral evidence, chapter 5 deals with documentary evidence and chapter 6 deals with circumstances when documentary evidence has been given preference over the oral evidence.

The last part, that is part 3, consists of chapter 7 to chapter 11. Chapter 7 talks about the burden of proof. Chapter 8 talks about estoppel, chapter 9 talks about witnesses, chapter 10 talks about examination of witnesses, and last chapter which is chapter 11 talks about improper admission and rejection of evidence.

The Indian Evidence Act Classification

In the Evidence Act All the Provisions can be divide in to two Categories (1) Taking the Evidence (By Court) (2) Evaluation

In Taking the Evidence Court take the Evidence for the Facts (Either “Issue of Facts” or “Relevant Facts”); The Facts means the things which is said before the court in connection with the matter, The main thing, which is Crime in Criminal and Right etc. in Civil matters are main Issues, So main Issues are known as “Issue of Facts”, and the other facts which are Relevant to it are “Relevant Facts”.

For those Facts Evidence is Given to the Court by two ways, One is orally and Second is Documentary (includes Electronic Documents), Oral Evidence mostly suggest the Verbal deposition before the Court (and not otherwise), and which includes oral statement regarding materials too, Documentary Evidence suggest the Documents. So, The Evidence Regarding

Matter which have number of Facts, for which Evidence by way of oral or Documentary produced before the court for its Evaluation for either one fact or facts. Court by going throw those Documentary Evidence and Oral Evidence decide that particular fact and all facts are proved or not, or whether the fact or facts can be presumed to be proved?

In Evaluation as above said by looking in to the Oral and Documentary Evidence Court decide whether particular fact is proved or not, or facts are proved or not, In Evaluation there are two concepts to prove facts; One is Prove (Prove, Disprove or Not prove) and Other is Presumption (that fact is proved) (may Presume, Shall presume and Conclusive proof) After going to Oral and Documentary Evidence Court see that whether any fact or facts are proved by looking to such evidence or not? If at all no evidence is given or enough evidence is given for the fact it's said fact is 'Not proved'; The second Concept for evaluation is "Presumption" In Evidence many Section suggest these presumptions, Where there is said Facts 'may presume', Court is extremely free to believe it or not and may ask to prove the fact, In 'shall presume' there is more weight given to believe facts but in that too court may ask to give more evidence to prove the facts, Where in any provision it is said that particular fact, or particular fact in particular circumstances must be concluded as "conclusive proof' Court has no liberty then to believe it to be proved.

Classification of Evidence Act in Four Questions

Evidence Act may be divided in four questions.

Question 1 Evidence is Given of What

Answer 1 of Facts ("Issue of Facts" or "Relevant Facts")

Question 2 How the Evidence of such Facts are Given

Answer 2 The Evidence of Such Facts is given either by way of "Oral Evidence" or "Documentary Evidence'

Question 3 On whom the Burden to Prove Facts lies

Answer 3 "Burden of Proof" (of particular fact) or "Onus of proof" (to prove whole case)

Question 4 What is the Evaluation of the Facts?

Answer 4 The Evaluation is "Prove" or "Presumption" (of prove); the fact is either 'prove',' disprove', or 'Not prove'; or there may be presumption that prove of facts "may presume', 'shall presume', or 'conclusive proof'.

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. "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."

5. 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.

PMLA envisages designation of one or more courts of sessions as Special Court or Special Courts to try the offences punishable under PMLA and offences with which the accused may, under the Code of Criminal Procedure 1973, be charged at the same trial. PMLA allows Central Government to enter into an agreement with Government of any country outside India for enforcing the provisions of the PMLA, exchange of information for the prevention

of any offence under PMLA or under the corresponding law in force in that country or investigation of cases relating to any offence under PMLA.

As per the Section 3 of the Prevention of Money-Laundering Act, 2002, the offence of Money-Laundering is defined as under:

"Whosoever

- Directly or indirectly,
- Attempts to indulge, or
- Knowingly assists, or
- Knowingly is party, or
- is actually involved in
    - O any process, or
    - O activity connected,
- With the **Proceeds of Crime**, including it's
    - O Concealment,
    - O Possession,
    - O Acquisition or use; and
- Projecting or claiming it as **Untainted Property** shall be guilty of offence of Money-Laundering."

The definition of "Money-Laundering" in India is comprehensive enough to cover most of the instances of converting the black money into white, as the same will depend upon the willingness of Enforcement Authorities for strong implementation of, which is in any case subject to judicial scrutiny. Some of the examples of Money-Laundering in the corporate world cover the instances relating to Shell Companies, Foreign Investments, Corporate Mismanagement, Insider Trading and Bribery.

Proceeds of Crime

The term **"PROCEEDS OF CRIME"**, which is an essential ingredient of Money-Laundering has been defined under Section 2(u) of PMLA, and it means and includes

- Any property derived or obtained

- Directly or indirectly
- By any person
- As a result of criminal activity
- relating to a
- scheduled offense or
- Value of any such property.

It is only when proceeds of crime are projected or claimed as untainted property i.e. uncorrupted; the offense of Money-Laundering is committed.

Methods and Means for financial fraud

Some of the ways for generation of black money which are peculiar to the Corporate Sectors may be narrated herein below:

- External Trade and Transfer Pricing;
- Manipulation by Way of International Transactions through Associate Enterprises;
- Financial Market Transactions;
- Out of Book Transactions;
- Parallel Books of Accounts;
- Manipulation of Books of Account;
- Manipulation of Sales/Receipts;
- Under-reporting of Production;
- Manipulation of Expenses;
- Manipulations of Accounts;
- Manipulation of Capital;
- Manipulation of Closing Stock;
- Manipulation of Capital Expenses;
- Generation of Black money in Some Vulnerable Sections of the Economy;
- Land and Real Estate Transactions;

- Bullion and Jewellery Transactions;
- Public Procurement;
- Non-profit Sector;
- Informal Sector and Cash Economy;
- Investment through Innovative Derivative Instruments.

Under PMLA, committing any offenses as specified in the Part A and Part C of the Schedule of PMLA, will invoke the provisions of PMLA. Some of the Acts and offences, which may attract PMLA, are enumerated herein below:

- An offence which is the offence of Cross Border implications and is specified in Part a of Schedule under PMLA, or
- The offences against property under Chapter XVII of the Indian Penal Code is applicable, involving cross border implications.
- Offences under the
    - O The Indian Penal Code, 1860 including offences relating to Cheating, Counterfeiting of Government stamps, Dishonest or Fraudulent removal or Concealment of Property to prevent distribution among creditors, dishonestly or fraudulently preventing debt is available for creditors, Dishonest or Fraudulent execution of deed of transfer containing false statement of consideration.
    - O Offences under the Narcotic Drugs and Psychotropic Substances Act, 1985
    - O Offences under the Prevention of Corruption Act, 1988;
    - O Offences under the Securities and Exchange Board of India Act, 1992 including offences relating to
        - Prohibition of manipulative and deceptive devices,
        - Insider trading and substantial Acquisition of securities or control.
    - O Offences under the Customs Act, 1962 relating to evasion of duty or prohibitions;
    - O Offences under the Emigration act, 1983
    - O Offences under the Foreigners act, 1946

- O Offences under the Antiquities and Arts Treasures Act, 1972
- O Offences under the Copyright Act, 1957, including
  - Offence of infringement of copyright or other rights conferred by Copyright Act.
  - Knowing use of infringing copy of computer programme;
- O Offences under the Trade Marks Act, 1999 including
  - Application of false trademarks, trade descriptions, etc.
  - Selling goods or providing services to which false trademark or false trade description is applied.
  - Falsely representing a trade mark as registered.
  - Abetment in India of acts done out of India.
- O Offences under The Information Technology Act, 2000, including
  - Breach of confidentiality and privacy,
  - Offence or contravention committed outside India.
- O Offences under the Suppression of Unlawful Acts against Safety of Maritime Navigation and Fixed Platforms on Continental Shelf Act, 2002

Offences by Companies

Section 70 of PMLA deals with offences by Companies, providing that Where a person committing a contravention of any of the provisions of this Act or of any Rule, Direction or Order made there under is a Company (company" means anybody corporate and includes a firm or other association of individuals); and

- Every person who, at the time the contravention was committed, was
  - O in charge of, and
  - O was responsible to the company,
    - For the conduct of the business of the company
    - As well as the company,

Shall be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished under PMLA.

The only exception to such rule is that if such person proves that the contravention took place

- Without his Knowledge, or
- That he exercised all due diligence to prevent such contravention.

Further, notwithstanding anything contained in sub-section (1) of Section 70 of PMLA, where a contravention of any of the provisions of this Act or of any Rule, Direction or Order made there under has been committed by a company and it is proved that the contravention has taken place

- With the consent or connivance of, or
- is attributable to any neglect on the part of any Director, Manager, Secretary or other Officer of any Company,

Such Director, Manager, Secretary or other Officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Obligations of Banking Companies, Financial Institutions and Intermediaries

Under Section 12 of PMLA, all Banking Companies, Financial Institutions And Intermediaries are required to maintain a record of all transactions, including information relating to transactions for a period of 5 years, in such manner as to enable it to reconstruct individual transactions, and furnish to the concerned Authorities under PMLA, all information relating to such transactions, whether attempted or executed; the nature and value of such transactions; verify the identity of its clients and the beneficial owner, if any; and maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

Punishment under PMLA

Section 4 of PMLA prescribes the Punishment for Money-Laundering as under:

- Rigorous Imprisonment for a term
  - O which shall not be less than Three years, but
  - O which may extend to 7 years/10 years, and
  - O shall also be liable to fine.

In certain cases, the offences under Narcotic Drugs and Psychotropic Substances Act, 1985 are punishable with rigorous imprisonment up to 10 years. The fine under PMLA is without any limit and the same may be commensurate to the nature and extent of offence committed and the money laundered.

Arrests

Under Section 19 of PMLA, the appropriate authority under the Act has the power to arrest any person provided that such authority on the basis of the material in his possession has reason to believe that such person has been guilty of any offence punishable under PMLA. After the arrest, the person arrested has to be informed about the grounds for his arrest. It is also required that the person so arrested shall, within 24 hours, be produced before the Judicial Magistrate or a Metropolitan Magistrate, as the case may be, having jurisdiction.

Attachment, Adjudication and Confiscation

Under Section 5 of PMLA, if the authority as specified under the Section, has reason to believe (the reason for such belief to be recorded in writing), on the basis of material in their possession, that-

- Any person is in possession of any Proceeds of Crime; and
- Such Proceeds of crime are likely to be
    - O Concealed,
    - O Transferred, or
    - O dealt with in any manner
        - Which may result in frustrating any proceedings relating to confiscation of such Proceeds of Crime?

May, by order in writing, provisionally attach such property for a period not exceeding 180 days from the date of the order, in such manner as may be prescribed.

Attachment of 3rd Party Properties

Under PMLA, even the property of any person may be attached under Section 5(1) 2nd Proviso, if the designated officer has reason to believe that the property in possession of such person is involved in Money-Laundering, and the non-attachment will frustrate any proceedings under the Act.

However, nothing in Section 5 of PMLA shall prevent the person interested in the enjoyment of the immovable property attached from such enjoyment. “Person interested”, in relation to any immovable property, includes all persons claiming or entitled to claim any interest in the property.

What after the Attachment of Property?

Section 8 of PMLA provides an elaborate procedure for adjudication of a complaint under Section 5 of PMLA, and a person holding property on behalf of any other person, or if there is a claim by a third person not a party to the complaint, such person is also required to be implicated into the proceedings for adjudication, and heard by the Adjudicating Authority.

Presumptions and Burden of Proof

Where Money-Laundering involves two or more inter-connected transactions and one or more such transactions is or are proved to be connected with Money-Laundering, then for the purposes of Adjudication or Confiscation, under Section 8 or for the trial of the Money-Laundering offence, it shall unless otherwise proved, be presumed that the remaining transactions form part of such inter-connected transactions associated with Money- Laundering

Under Section 24 of PMLA, in any proceeding relating to the proceeds of crime a presumption is raised by the authority or court against any person charged with the offence of Money-Laundering, unless the contrary is proved by the accused, that such proceeds of crime are involved in money-laundering; and in the case of any third person, such authority or court **may** also presume that such proceeds of crime are involved in Money-Laundering.

Essentially, under PMLA, the burden of proof lies on the person who claims that the proceeds of crime alleged to be involved in Money-Laundering, are not involved in Money-Laundering. The presumption against the accused or any 3rd party is good enough to discharge the onus of the authorities under PMLA. Even in the case of Records, and Properties, which are found in the possession or control of any person in the course of a survey or search under the Act (Section 16, Section 17 and Section 18 of PMLA), under a presumption is raised that such records or property belongs to such person, and the contents of such records are true, and further that signatures and any part of such records in hand-writing of a particular person or in the hand-writing of such person, the presumptions as to the records in property are absolute, and the onus to prove the same otherwise, lies on such person.

It is clear that, a person accused of an offence under Section 3 of PMLA, whose property is attached and proceeded against for Confiscation, shall discharge the onus of proof (Section 24) vested in him by disclosing the sources of his Income, Earnings or Assets, out of which or means by which he has acquired the property attached, to discharge the burden that the property does not constitute proceeds of crime.

Where a transaction of acquisition of property is part of inter-connected transactions, the onus of establishing that the property acquired is not connected to the activity of Money-Laundering, is on the person in ownership, control or possession of the property, though not accused of a Section 3 offence under PMLA, provided one or more of the interconnected transactions is or are proved to be involved in Money-Laundering (Section 23).

6. 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 authorised person to deal in foreign exchange or foreign security. Such an authorised 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 authorised 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.

VARIOUS COMMITTEES

Santhanam Committee

That there were some functional inadequacies in the IPC was recognized by the Santhanam Committee (1962) which observed that ‘the Penal Code does not deal in any satisfactory

manner with acts which may be described as social offences having regard to special circumstances under which they are committed and which have now become a dominant feature of certain powerful sections of modern society.'

Mitra Committee

An Experts Committee on Legal Aspects of Bank Frauds appointed by Reserve Bank of India headed by Sri NL Mitra in its report submitted in 2001 recommended that financial fraud needs to be criminalized by inserting a definition for the offence on 'financial fraud' and a penal provision in the Indian Penal Code.

Second Administrative Reforms Commission

The Second Administrative Reforms Commission (2005) in its Fourth report on Ethics in Governance made the following recommendations, including reiterating Mitra Committee recommendation, with reference to Serious Economic Offences:

a. A new law on 'Serious Economic Offences' should be enacted.

b. A Serious Economic Offence may be defined as:

   I. One which involves a sum exceeding Rs 10 crore; or

   Ii. is likely to give rise to widespread public concern; or

   iii. Its investigation and prosecution are likely to require highly specialized knowledge of the financial market or of the behaviour of banks or other financial institutions; or

   iv. Involves significant international dimensions; or

   V. in the investigation of which there is requirement of legal, financial, investment and investigative skills to be brought together; or

   vi. Which appear to be complex to the Union Government, regulators, banks, or any financial institution?

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. State vigilance Commission

viii. Lokayuktha & UpaLokayuktha

Serious Fraud Investigation Office

http://sfio.nic.in/websitenew/main2.asp

The SFIO is a non-statutory body and was set up on the basis of the recommendations of the Naresh Chandra Committee on corporate governance in the backdrop of stock market scams, failure of non-financial banking companies and the phenomena of vanishing companies and plantation companies. It is a multi-disciplinary organization with experts on finance, capital market, accountancy, Forensic Investigation, taxation, law, information technology, company law, customs and investigation. These experts are drawn from banks, the Securities and Exchange Board of India (SEBI), the Comptroller and Auditor General's office and the organizations and departments concerned of the government.

The SFIO will normally take up for investigation only such cases, which are characterized by

- Complexity and having inter-departmental and multi-disciplinary ramifications;
- substantial involvement of public interest to be judged by size, either in terms of monetary misappropriation or in terms of persons affected, and;

- The possibility of investigation leading to or contributing towards a clear improvement in systems, laws or procedures. The SFIO shall investigate serious cases of fraud received from Department of company Affairs.

SFIO does not initiate any investigation on its own, based on any complaints/documents received from any source. The cases are taken up for investigation as are order for investigation by the Government i.e. Ministry of Corporate Affairs under the Companies Act, 2013. These provisions enable the Central government to appoint one or more competent persons as inspectors to investigate and submit a report on the affairs of a company if, in its opinion, or in the opinion of the Registrar of Companies or the Company Law Board, there are circumstances suggesting that the business of a company is being conducted with the intention to defraud its creditors or members, or for a fraudulent or unlawful purpose.

12 FORENSIC INVESTIGATION UNDER THE INFORMATION TECHNOLOGY ACT, 2000

THE INFORMATION TECHNOLOGY ACT, 2000 is an Act to provide legal recognition for 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 filing of documents with the Government agencies and further to amend the Indian Penal Code, the 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 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 provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures. It also defines cyber crimes and prescribes penalties for them. The Act directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures. It also established a Cyber Appellate Tribunal to resolve disputes arising from this new law. The Finance Act, 2017, merged the Cyber Appellate Tribunal with the Telecom Disputes Settlement and Appellate Tribunal with effect from 26 May 2017.The Act also amended various sections of the Indian Penal Code, 1860,

the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934 to make them compliant with new technologies.

Amendments [

A major amendment was made in 2008. It introduced Section 66A which penalized sending of "offensive messages". It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced provisions addressing child porn, cyber terrorism and voyeurism. The amendment was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed into law by President Pratibha Patil, on 5 February 2009. The amendments came into effect from 27 October 2009.

Offences sections

- **Section 65 – Tampering with Computer Source Documents** If any person knowingly or intentionally conceals, destroys code or alters or causes another to conceal, destroy code or alter any computer, computer program, computer system, or computer network, he shall be punishable with imprisonment up to three years, or with fine up to two lakh rupees, or with both.
- **Section – 66 Computer Related Offences** If any person, dishonestly, or fraudulently, does any act referred to in section 43,he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.
- **Section 66A – Punishment for sending offensive messages through communication service**

  Any person who sends, by means of a computer resource or a communication device,
  - Any information that is grossly offensive or has menacing character;
  - Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,

- Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages

Shall be punishable with imprisonment for a term which may extend to three years and with fine.

- **Section 66B – Punishment for dishonestly receiving stolen computer resource or communication device.** Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.
- **Section 66C – Punishment for identity theft** Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.
- **Section 66D – Punishment for cheating by personation by using computer resource** Whoever, by means of any communication device or computer resource cheats by personating; shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.
- **Section 66E – Punishment for violation of privacy** Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, Explanation – For the purposes of this section:
    a. "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;
    b. "capture", with respect to an image, means to videotape, photograph, film or record by any means;

c. “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

d. “publishes” means reproduction in the printed or electronic form and making it available for public;

e. “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that–

i. he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

ii. Any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

- **Section-66F Cyber Terrorism**

- Whoever,-

a. with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

i. denying or cause the denial of access to any person authorized to access computer resource; or

ii. attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

iii. introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

b. knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of

such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

- Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

- **Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.-**

1. Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.
2. The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
3. The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to –
    - provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

- intercept or monitor or decrypt the information, as the case may be; or
- Provide information stored in computer resource.

4. The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

- **Section 69A – Power to issue directions for blocking for public access of any information through any computer resource**

5. Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.
6. The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.
7. The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

- **Section 69B. Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security**

8. The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
9. The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable

online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

10. The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
11. Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

- **Section 71 – Penalty for misrepresentation** Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
- **Section 72 – Breach of confidentiality and privacy** Any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
- **Section 72A – Punishment for Disclosure of information in breach of lawful contract** Any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

- **73. Penalty for publishing electronic Signature Certificate false in certain particulars.**

12. No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that

    a. the Certifying Authority listed in the certificate has not issued it; or

    b. the subscriber listed in the certificate has not accepted it; or

    c. the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation

    Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

- **Section 74 – Publication for fraudulent purpose:** Whoever knowingly creates publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
- **Section 75 – Act to apply for offence or contraventions committed outside India**

    Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

    For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

13. **Forensic Investigation under the Insolvency and Bankruptcy Code, 2016**

The Insolvency and Bankruptcy Code, 2016, (referred to hereinafter as “the Code”) is the option resorted to by the financial and the operational creditors of a corporate debtor, in the cases of non-payment of debt due.

The Code not only prescribes the procedures to be followed in case of the insolvency/ non payment of dues of the debtor, it also describes the transactions that are prejudicial to the general interests of the stakeholders. The Code specifically deals with transactions which are preferential, undervalued, entered into with the purpose of defrauding the creditors or extortionate credit transactions.

The following sections of the Code deal with the specific transactions:

Section 43: Preferential Transactions

Section 47: Application by creditors in case of Undervalued Transactions

Section 49: Transactions defrauding creditors

Section 50: Extortionate Credit Transactions

As per the Code and the Regulations issued thereto, the insolvency professional, who works as the interim resolution professional, the resolution professional or the liquidator, as per the stage of ongoing resolution process, has to form an opinion, on or before the 75th day of the insolvency commencement date, whether the corporate debtor has been subjected to any preferential transactions, undervalued transactions, extortionate credit transactions or fraudulent transactions. If the resolution professional is convinced that such a transaction has taken place, he shall make a determination on or before the 115th day of the insolvency commencement date, under intimation to the Board and apply to Adjudicating Authority for appropriate relief on or before the 135th day.

PREFERENTIAL TRANSACTIONS

The Resolution professional or the liquidator, as the case may be, is of the opinion that the corporate debtor has, at any given time, given preference to any persons, he can apply to the Adjudicating Authority for the avoidance of such preferential transactions.

As per Section 45(2) of the Code, the corporate debtors shall be deemed to have given preference, when there is a transfer of property or an interest thereof of the corporate debtor, for the benefit of a creditor or a surety or guarantor for a financial/operational debt or other liabilities outstanding, and the transfer so made, puts the creditor,

guarantor or the surety in a better position than he would have been in the event of distribution of assets in accordance of Section 53.

Also, for the transaction to be termed as a preferential transaction, the above mentioned transfers should have been made to a related party, other than the employee, of the corporate debtor within the period of two years preceding the insolvency commencement date and for the parties other than the related party of the corporate debtor, such transaction should have been entered during the one year period, immediately preceding the insolvency commencement date.

Wherever a preferential transaction is proved, as per Section 44, the adjudicating authority may pass such an order, so as to reverse the effect of the preferential transaction and require the interests in the property restored to the corporate debtor.

The provision to the section states that any order under this section shall not affect any interest in property which was acquired from a person other than the corporate debtor or any interest derived from such interest and was acquired in good faith and for value and require a person, who received a benefit from the preferential transaction in good faith and for value to pay a sum to the liquidator or the resolution professional.

Also, the explanations to the section 44 clarifies that, where a person, who has acquired an interest in property from another person other than the corporate debtor, or who has received a benefit from the preference or such another person to whom the corporate debtor gave the preference, had sufficient information of the initiation or commencement of insolvency resolution process of the corporate debtor or is a related party, it shall be presumed that the interest was acquired, or the benefit was received otherwise than in good faith unless the contrary is shown.

It is also clarified that a person shall be deemed to have sufficient information or opportunity to avail such information if a public announcement regarding the corporate insolvency resolution process has been made under section 13.

UNDERVALUED TRANSACTIONS

As per section 45 of the Code, a transaction shall be considered undervalued where the corporate debtor makes a gift to a person; or enters into a transaction with a person which involves the transfer of one or more assets by the corporate debtor for a consideration the value of which is significantly less than the value of the consideration

provided by the corporate debtor, and such transaction has not taken place in the ordinary course of business of the corporate debtor.

For such transaction, to be declared void and the effect of the transaction to be reversed, the transaction should have occurred within a period of one year prior to the commencement of the insolvency resolution process. In case of the occurrence of such transaction with the related party, the period covered is of two years preceding the insolvency commencement date.

If the liquidator or the resolution professional, as the case may be, on an examination of the transactions of the corporate debtor determines that certain transactions were made during the relevant period, as mentioned in above para, which were undervalued, he shall make an application to the Adjudicating Authority to declare such transactions as void and reverse the effect of such transaction.

The Adjudicating Authority may require an independent expert to assess evidence relating to the value of the transactions in case of undervalued transactions.

The Code, in case of undervalued transactions, if the liquidator or the resolution professional has not reported such transactions to the Adjudicating Authority, a creditor, member or a partner of a corporate debtor, as the case may be, may make an application to the Adjudicating Authority to declare such transactions void and reverse their effect in accordance with section 47 of the Code.

On examination of such application, If the Adjudicating Authority is satisfied that undervalued transactions had occurred and the liquidator or the resolution professional, as the case may be, after having sufficient information or opportunity to avail information of such transactions did not report such transaction to the Adjudicating Authority, it shall pass an order restoring the position as it existed before such transactions and reversing the effects thereof. It shall also require the Board to initiate disciplinary proceedings against the liquidator or the resolution professional as the case may be.

TRANSACTIONS DEFRAUDING CREDITORS

Section 49 of the Code provides that, where the corporate debtor has entered into an undervalued transaction as referred to in section 45(2) of the Code, and the Adjudicating Authority is satisfied that such transaction was deliberately entered into by

such corporate debtor for keeping assets of the corporate debtor beyond the reach of any person who is entitled to make a claim against the corporate debtor in order to adversely affect the interests of such a person in relation to the claim, the Adjudicating Authority shall make an order restoring the position as it existed before such transaction as if the transaction had not been entered into and protecting the interests of persons who are victims of such transactions.

But the section also provides that an order under this section shall not affect any interest in property which was acquired from a person other than the corporate debtor and was acquired in good faith, for value and without notice of the relevant circumstances, or affect any interest deriving from such an interest and shall not require a person who received the benefit from the transaction in good faith, for value and without notice of the relevant circumstances to pay any sum unless he was a party to the transaction.

EXTORTIONATE CREDIT TRANSACTIONS

Section 50 of the Code provides that, where the corporate debtor has been a party to an extortionate credit transaction involving the receipt of financial or operational debt during the period within two years preceding the insolvency commencement date, the liquidator or the resolution professional as the case may be, may make an application for avoidance of such transaction to the Adjudicating Authority if the terms of such transaction required exorbitant payments to be made by the corporate debtor.

The explanation to the section also clarifies that any debt extended by any person providing financial services which is in compliance with any law for the time being in force in relation to such debt shall in no event be considered as an extortionate credit transaction.

On examination of such application, if the Adjudicating Authority is satisfied that the terms of a credit transaction required exorbitant payments to be made by the corporate debtor, it shall pass an order to restore the position as it existed prior to such transaction. It may also, by order, set aside the whole or part of the debt created on account of the extortionate credit transaction or modify the terms of the transaction. The Adjudicating Authority may require any person who is, or was, a party to the transaction to repay any amount received by such person or require any security interest that was created as part of the extortionate credit transaction to be relinquished in favour of the liquidator or the resolution professional, as the case may be.

PENALTIES/ PUNISHMENTS FOR DEFRAUDING CREDITORS

Section 69 of the Code provides for penalties and punishments to the officers of the corporate debtor or the corporate debtor itself, in case of their involvement in the transactions for defrauding the creditors.

If an officer of the corporate debtor or the corporate debtor shall be punishable with imprisonment for a term which shall not be less than one year, but which may extend to five years, or with fine which shall not be less than one lakh rupees, but may extend to one crore rupees, or with both, if he has been involved in any transaction undertaken so as to defraud the creditors or affect their interest in adverse manner. But a person shall not be punishable under this section if the said acts were committed more than five years before the insolvency commencement date; or if he proves that, at the time of commission of those acts, he had no intent to defraud the creditors of the corporate debtor.

The punishment and penalty are also applicable in the case of concealment or removal of any part of the property of the corporate debtor within two months before the date of any unsatisfied judgment, decree or order for payment of money obtained against the corporate debtor.

Section 73 contains penalties and punishments in the case of the corporate debtor or any officer thereof, makes false representations to the creditors. The punishment under this section is imprisonment for a term which shall not be less than three years, but may extend to five years or with fine which shall not be less than one lakh rupees, but may extend to one crore rupees, or with both.

Section 73 is applicable when any officer of the corporate debtor on or after the insolvency commencement date, makes a false representation or commits any fraud for the purpose of obtaining the consent of the creditors of the corporate debtor or any of them to an agreement with reference to the affairs of the corporate debtor, during the corporate insolvency resolution process, or the liquidation process or prior to the insolvency commencement date, has made any false representation, or committed any fraud, for that purpose.

Also, Section 235A of the Code provides for punishments in situations where no specific penalty has been provided. As per the section, if any person contravenes any of

the provisions of this Code or the rules or regulations made thereunder for which no penalty or punishment is provided in this Code, such person shall be punishable with fine which shall not be less than one lakh rupees but which may extend to two crore rupees.

To determine whether such transactions defrauding the creditors and other stakeholders have taken place, it is of utmost importance to undertake a forensic investigation

14. Forensic Investigationunder 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 anybody 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,
- "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.

15. Forensic Investigation of Listed Corporate Entities

The forensic investigation is ordered in the cases of financial frauds, to recover the defrauded assets and to gather enough unquestionable evidence to be presented before the court of law, so as to punish the wrong-doer.

The forensic investigation can be ordered by regulators like the Ministry of Corporate Affairs, the Securities and Exchange Board of India or the respective stock exchange where the company has been registered.

The forensic investigation can also be ordered internally, by the board of directors of the company, for purposes of internal control and to identify any lapse thereto.

Listed below is the checklist of activities to be performed by the forensic investigator in case of a forensic investigation assignment.

In case of internal investigation, appointment letter and scope of work from the company should be studied and understood in detail.

In case of statutory appointment, following documents should be collected and studied, before the initiation of the assignment.

- Letter of appointment from the regulators
- Scope of work
- Any instructions as to the methods of investigations to be implemented or any specific accounts to be verified in depth.
- Any orders passed by SEBI
- Collect all the letters and replies submitted to SEBI, before the order was passed.
- Study all the letter and replies submitted to all the applicable authorities by the company under investigation.
- Collect as much information as possible on the industry in which the company functions and the general norms of the industry.

Research the company on MCA portal

- Collect all possible details about the company from the filings made with the BSE and MCA portals.
- Run a check on other directorships and commitments of all the directors and KMPs of the auditee.
- Check whether there are any transactions between the company under investigation and the company which has common directors with it.
- If there are any transactions entered into, check those transaction in detail.
    - Are the transactions in normal course of business?
    - Are the transactions undertaken at arm's length prices?
    - Had the transactions reported in the books, actually taken place or are merely book entries? Collect enough documentary evidence for the same.
    - Were the companies with common directors, ever reported as related party?
- Check the financials and other details of the companies with common directors with the company under investigation. Are there any suspicious transactions?
- Are there any subsidiary companies or joint ventures? If yes, verify the financials and other details of the same.

Check the legal compliances

- Has the company complied with the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015?
- Are the provisions of the Companies Act, 2013 complied with? Specific focus required on the explanation to Section 134(5) (e) of the Act.
- The Companies Act, 2013, covers directors responsibility under section 134(5), responsibility of the auditors u/s 143 and that of the company secretaries u/s 205, 206. Have these sections been complied with?
- Has the company complied with all the applicable accountings, cost accounting, auditing and secretarial standards?
- Are the Auditing and Assurance standards followed by the auditors in carrying out their assignment and preparation of reports?
- Is the functioning of the company in line with its incorporation documents?
- Are the compliances of general laws and laws specific to the industry complied with?
- Are there any disputes with any authorities?
- Are there any payments due to be made to any of the authorities outstanding?
- Are applicable labour laws, business laws, taxes on income, VAT, GST, etc. wherever applicable, have been followed and all compliances as per those acts done in a timely manner?
- Does the company require any permissions from any authorities to carry out its business? Has such permissions been taken?
- Are there any ongoing cases for /against the company under investigation with any of the authorities? If yes, current status of the case and future action proposed to be taken.
- Is the appointment of all the officials, including directors and KMPs within the ambit of law? Are there any discrepancies? Proper documentation of appointment entered into?

Meetings with company officials

- Understand the business model and the functioning of the company. Ask questions to get information. Frame questions in such a manner that each question extracts maximum possible information.
- Understand what the company officials have to say with respect to the investigation being conducted.

- Ask for internal financial control policy and understand the same.
- The meeting with the directors, chief financial officer, compliance officer and company secretary of the company, practicing company secretary, statutory auditors, internal auditors, should be held separately. Each should be asked to prove that they have disposed of their duties in the best possible manner and there has been no lapse from their end.
- Has the company formed requisite committees of the board? Are the meetings of the board and the committees held as per the requirements of the law at regular time intervals? Is the composition of the committee as per the legal requirements?

Checking of the books and registers of the auditee:

All the principles and guidelines of internal and statutory audit are applicable to the forensic investigation assignment.

- Make a list of all the books and registers that the company is required to maintain.
- Verify all the registers and books that are required to maintain.
- Check the agenda, agenda notes, notices and minutes of the meetings of the Board of Directors and other board committees. See if all the provisions related thereto are complied with and there are no discrepancies.
- Ledger scrutiny of the books of accounts.
- Collect the yearly financial statements, annual report, tax audit report, secretarial audit report, cashflow statements of the company under investigation.
- Collect and verify all the contracts entered into by the company. Proper documentation for all the loans taken or advances made, documents for day to day purchase/sale/provision of services, etc.
- In case of loans and advances, verify that they are made in the due course of business at rates of interest in line with the existing market rates and the said transactions are not prejudicial to the business as a whole or to any class of stakeholders in particular.
- Verify that all the accounts making up the total trade receivables and payables are active and not dormant.
- Verify that all the transactions are reported in the books of accounts and no transactions are directly set off against one another, without bringing them to the books.

- Verify the fixed assets register and also physically verify the fixed assets.
- Verify the share capital account and see if there are any new issues of shares, debentures, preferential allotment, rights issue, etc. If any such issues are made, check if proper procedures were followed and all the statutory compliances made. Thereafter verify how much fund was raised and where is it used/proposed to be used.
- Check the reserves account. If there are accumulated losses, dig out the information on the same, as in when were the losses incurred? Reason for the loss, if it is ongoing, what steps has the management taken in order to reduce the losses and to keep them in check.
- Verify the items falling under the head current liabilities.
- Check whether there are any contingent liabilities. Gather information as to the chances of contingent liability becoming a liability and if they should be reclassified.
- Are investments shown at fair value?
- Verify whether appropriate provisions are made for probable losses.

In forensic investigation, before a report can be made or an opinion be expressed, it is of utmost importance for the investigator, to know the business of the company and all the events that have occurred during its life, like the back of his hand. With the company knowledge and appropriate technical knowledge of the laws of the land, a forensic investigation can be successfully completed.

PART III

17. ROLE OF FORENSIC ACCOUNTANTS

Forensic accounting requires the most important quality a person can possess: the ability to think. There is no book that tells you how to do a forensic investigation. It is about solving a puzzle or peeling an onion. It takes creativity. All of the larger accounting firms, as well as many medium-sized and boutique firms, have specialist forensic accounting departments. Within these groups, there may be further sub-specializations: some forensic accountants

may, for example, just specialize in insurance claims, personal injury claims, fraud, construction, or royalty audits. Forensic accountants may be involved in recovering proceeds of crime and in relation to confiscation proceedings concerning actual or assumed proceeds of crime or money laundering. In the United Kingdom, relevant legislation is contained in the Proceeds of Crime Act 2002. In India there is a separate breed of forensic accountants called Certified Forensic Accounting Professionals. Some forensic accountants are also Certified Fraud Examiners, Certified Public Accountants, or Chartered Accountants. Forensic accountants utilize an understanding of business information and financial reporting systems, accounting and auditing standards and procedures, evidence gathering and investigative techniques, and litigation processes and procedures to perform their work. Forensic accountants are also increasingly playing more proactive risk reduction roles by designing and performing extended procedures as part of the statutory audit, acting as advisers to audit committees, fraud deterrence engagements, and assisting in investment analyst research. The forensic Accountant is a bloodhound of Bookkeeping. These bloodhounds sniff out fraud and criminal transactions in bank, corporate entity or from any other organization's financial records. They hound for the conclusive evidences. External Auditors find out the deliberate misstatements only but the Forensic Accountants find out the misstatements deliberately. External auditors look at the numbers but the forensic auditors look beyond the numbers. Forensic accountant takes a more proactive, skeptical approach in examining the books of Accounting. They make no assumption of management integrity (if they can assume so then there is no need for their appointment) show less concerns for the arithmetical accuracy have nothing to do with the Accounting or Assurance standards but are keen in exposing any possibility of fraud. In addition to the specialized knowledge about the techniques of finding out the frauds one needs patience and analytical mindset. One has to look beyond the numbers and grasp the substance of the situation. It is basically the work of the intelligent accountants. He needs to question seemingly benign document and look for inconsistencies. He searches for evidence of criminal conduct or assists in the determination of, or rebuttal of, claimed damages.

In the Indian context the Forensic Accountants are the most required in the wake of the growing frauds. After the Satyam scam, forensic auditors are much in demand as many companies want to understand what could be the initial warning signals of a Satyam kind of

fraud in other Indian companies. Even the government's Serious Fraud Investigation Office (SFIO) has sought the help of forensic accountants to get to the root of the financial fraud at Satyam.

Forensic accountants are trained to detect evidence of frauds. Forensic accounting is about more than legal matters and financial numbers. There is an acute shortage of forensic accounting skill sets in India. A huge demand for forensic accountants has come up in the wake of the requirements from the investors after the Satyam fiasco. There are only about 400 forensic accountants in the country though India loses approximately $40 billion because of frauds.

18. CYBER CRIME & SECURITY STRATEGY FOR CYBER CRIME

Businesses are increasingly the victims of cyber-attacks. These crimes are not only costly for the companies, but can also put their very existence at risk and may provoke significant externalities for third parties. The World Federation of Exchanges reported in July 2013 that half of the 46 exchanges it surveyed had been victims of cyber-attacks in the previous year. In a 2013 Financial Times article, the Depository Trust and Clearing Corporation, which processes large securities transactions for U.S. capital markets, described cybercrime "as arguably the top systemic threat facing global financial markets and associated infrastructure."

Cybercrime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cybercrime 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 cybercrimes when the illegal activities are committed through the use of a computer and the Internet.

The first recorded cybercrime 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 1976 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 Skeena, developed the EIK Cloner.

Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones.

Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, extortion, child pornography, and child grooming.

Cyber crime violates privacy and confidentiality of information by intercepting or disclosing it lawfully or unlawfully. Cybercrimes are sometimes defined from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones".

Cybercrimes are not just restricted to individualsand businesses, internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation state is sometimes referred to as cyber warfare

CYBER CRIME encompasses are large variety of crimes. Some of them are discussed below

1. **Financial fraud crimes**

Computer fraud or Internet fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;
- Altering or deleting stored data;

Other forms of financial fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information. These types of crime often result in the loss of private information or monetary information.

Cyberterrorism

Government officials and information technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. Such intrusions are part of an organized effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical systems.A cyberterrorist is someone who intimidates or coerces a government or an organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.

Cyberterrorism in general can be defined as an act of terrorism committed through the use of cyberspace or computer resources. As such, a simple propaganda piece in the Internet that there will be bomb attacks during the holidays can be considered cyberterrorism. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

Cyberextortion

Cyberextortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". The cybercrime extortionists attack corporatewebsites and networks, crippling their ability to operate and demanding payments to restore their service.

Cyber warefare is the use or targeting in a battlespace or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations pertaining to the threat of cyber attacks, espionage and sabotage.

The attack on Estonia's infrastructure in 2007, and the Ukraine power grid attack are cyberattacks that shook the world posing new threats to the severity of nations.

CATEGORIES OF CYBER CRIME

We can categorize cybercrime in two ways

- Computer as a target: Here the computers are used as target of crime**.** These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators e.g. Hacking, virus/worms' attacks, Dos attack, malware
- The computer as a weapon: When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychology and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend.

Crimes that use computer networks or devices to advance other ends include:

Hacking

Hacking in simple terms means illegal intrusion information a computer system and/or network. It is also known as cracking. Government websites are the hot target of the hackers due to the press coverage, it receives. Hackers enjoy the media coverage. Motive behind the

crime called Hackers Motive, hacking greed power, publicity, revenge, adventure desire to access forbidden information destructive mindset wants to sell network security services.

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.

Email 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 Section 417, 419 & 465 of 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. 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

Viruses and Trojans are harmful programs that are loaded onto your computer without your knowledge. The goal of these programs may be to obtain or damage information, hinder the performance of your computer, or flood you with advertising.

Viruses spread by infecting computers and then replicating. Trojans appear as genuine applications and then embed themselves into a computer to monitor activity and collect information.

Using a firewall and maintaining current virus protection software can help minimize your chances of getting viruses and inadvertently downloading Trojans.

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.

CYBER SECURITY

Cyber Security involves protection of sensitive personal and business information through prevention, detection and response to different online attacks.

Privacy Policy: Before submitting your name, e-mail, address, on a website look for the sites privacy policy.

Keep Software Up to Date: If the seller reduces patches for the software operating system your device, install them as soon as possible. Installing them will prevent attackers form being able to take advantage Use good password which will be difficult for thieves to guess. Do not choose option that allows your computer to remember your passwords.

Disable Remote Connectivity: Some PDA's and phones are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when they are not in use.

Advantages of Cyber Security

- Cyber security will defend us from critical attacks.
- It helps us to browse the site, website.
- Internet Security processes all the incoming and outgoing data on your computer.
- It will defend us from hacks and virus.
- Application of cyber security used in our PC needs update every week

Safety Tips to Cyber Crime

- Use antivirus Software
- Insert Firewalls
- Uninstall unnecessary software
- Maintain backup
- Check security settings

19. FORENSIC INVESTIGATION IN DIGITAL ENVIRONMENT

The modern digital environment offers new opportunities for both perpetrators and investigators of fraud. In many ways, it has changed the way fraud examiners conduct

investigations, the methods internal auditors use to plan and complete work, and the approaches external auditors take to assess risk and perform audits.

While some methods, such as online working papers, are merely computerized versions of traditional tasks, others, such as risk analysis based on neural networks, are revolutionizing the field. Many auditors and researchers find themselves working amid an ever-changing workplace, with computer-based methods leading the charge.

What are Digital Forensics?

Digital forensics (sometimes known as **digital forensic science**) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data. With roots in the personal computing revolution of the late 1970s and early ‘80s, the discipline evolved in a haphazard manner during the 1990s, and it was not until the early 21st century that national policies emerged.

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil (as part of the electronic discovery process) courts. Forensics may also feature in the private sector; such as during internal corporate investigations or intrusion investigation (a specialist probe into the nature and extent of an unauthorized network intrusion).

The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved; computer forensics, network forensics, forensic data analysis and mobile device forensics. The typical forensic process encompasses the seizure, forensic imaging (acquisition) and analysis of digital media and the production of a report into collected evidence.

As well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources (for example, in copyright cases), or authenticate documents. Investigations are much broader in scope than other areas of forensic analysis (where the usual aim is to provide answers to a series of simpler questions) often involving complex time-lines or hypotheses.

History

Prior to the 1980s crimes involving computers were dealt with using existing laws. The first computer crimes were recognized in the 1978 Florida Computer Crimes Act, which included legislation against the unauthorized modification or deletion of data on a computer system. Over the next few years the range of computer crimes being committed increased, and laws were passed to deal with issues of copyright, privacy/harassment (e.g., cyber bullying, cyber stalking, and online predators) and child pornography. It was not until the 1980s that federal laws began to incorporate computer offences. Canada was the first country to pass legislation in 1983. This was followed by the US Federal Computer Fraud and Abuse Act in 1986, Australian amendments to their crimes acts in 1989 and the British Computer Abuse Act in 1990.

Development of forensic tools

During the 1980s very few specialized digital forensic tools existed, and consequently investigators often performed live analysis on media, examining computers from within the operating system using existing sysadmin tools to extract evidence. This practice carried the risk of modifying data on the disk, either inadvertently or otherwise, which led to claims of evidence tampering. A number of tools were created during the early 1990s to address the problem.

The need for such software was first recognized in 1989 at the Federal Law Enforcement Training Centre, resulting in the creation of IMDUMP (by Michael White) and in 1990, Safe Back (developed by Side). Similar software was developed in other countries; DIBS (a hardware and software solution) was released commercially in the UK in 1991, and Rob McKemmish released Fixed Disk Image free to Australian law enforcement. These tools allowed examiners to create an exact copy of a piece of digital media to work on, leaving the original disk intact for verification. By the end of the ‘90s, as demand for digital evidence grew more advanced commercial tools such as En Case and FTK were developed, allowing analysts to examine copies of media without using any live forensics. More recently, a trend towards “live memory forensics” has grown resulting in the availability of tools such as Windows SCOPE.

More recently the same progression of tool development has occurred for mobile devices; initially investigators accessed data directly on the device, but soon specialist tools such as XRY or Radio Tactics Aceso appeared.

Forensic Process

A digital forensic investigation commonly consists of 3 stages: acquisition or exhibits, analysis, and reporting. Ideally acquisition involves capturing an image of the computer's volatile memory (RAM) and creating an exact sector level duplicate (or "forensic duplicate") of the media, often using a write blocking device to prevent modification of the original. However, the growth in size of storage media and developments such as cloud computing have led to more use of 'live' acquisitions whereby a 'logical' copy of the data is acquired rather than a complete image of the physical storage device. Both acquired image (or logical copy) and original media/data are hashed (using an algorithm such as SHA-1 or MD5) and the values compared to verify the copy is accurate.

There are four stages of forensics Process: -

1. Identification of Digital Evidence
2. Preservation of Digital Evidence
3. Analysis of Digital Evidence
4. Presentation of Digital Evidence

During the analysis phase an investigator recovers evidence material using a number of different methodologies and tools. In 2002, an article in the International Journal of Digital Evidence referred to this step as "an in-depth systematic search of evidence related to the suspected crime." In 2006, forensics researcher Brian Carrier described an "intuitive procedure" in which obvious evidence is first identified and then "exhaustive searches are conducted to start filling in the holes."

The actual process of analysis can vary between investigations, but common methodologies include conducting keyword searches across the digital media (within files as well as unallocated and slack space), recovering deleted files and extraction of registry information (for example to list user accounts, or attached USB devices).

The evidence recovered is analyzed to reconstruct events or actions and to reach conclusions, work that can often be performed by less specialized staff. When an investigation is complete the data is presented, usually in the form of a written report, in lay persons' terms.

Application

Digital forensics is commonly used in both criminal law and private investigation. Traditionally it has been associated with criminal law, where evidence is collected to support

or oppose a hypothesis before the courts. As with other areas of forensics this is often as part of a wider investigation spanning a number of disciplines. In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings (for example to locate, identify or halt other crimes). As a result, intelligence gathering is sometimes held to a less strict forensic standard.

In civil litigation or corporate matters digital forensics forms part of the electronic discovery (or e Discovery) process. Forensic procedures are similar to those used in criminal investigations, often with different legal requirements and limitations. Outside of the courts digital forensics can form a part of internal corporate investigations.

A common example might be following unauthorized network intrusion. A specialist forensic examination into the nature and extent of the attack is performed as a damage limitation exercise. Both to establish the extent of any intrusion and in an attempt to identify the attacker. Such attacks were commonly conducted over phone lines during the 1980s, but in the modern era are usually propagated over the Internet.

The main focus of digital forensics investigations is to recover objective held in digital devices can help with other areas of inquiry.

Attribution

Meta data and other logs can be used to attribute actions to an individual. For example, personal documents on a computer drive might identify its owner.

Alibis and statements

Information provided by those involved can be cross checked with digital evidence. For example, during the investigation into the Soham murders the offender's alibi was disproved when mobile phone records of the person he claimed to be with showed she was out of town at the time.

Intent

As well as finding objective evidence of a crime being committed, investigations can also be used to prove the intent (known by the legal term men's rea). For example, the Internet history of convicted killer Neil Entwistle included references to a site discussing How to kill people.

Evaluation of source

File artefacts and meta-data can be used to identify the origin of a particular piece of data; for example, older versions of Microsoft Word embedded a Global Unique Identifier into files which identified the computer it had been created on. Proving whether a file was produced on the digital device being examined or obtained from elsewhere (e.g., the Internet) can be very important.

Document authentication

Related to "Evaluation of source," Meta data associated with digital documents can be easily modified (for example, by changing the computer clock you can affect the creation date of a file). Document authentication relates to detecting and identifying falsification of such details.

Limitations

One major limitation to a forensic investigation is the use of encryption; this disrupts initial examination where pertinent evidence might be located using keywords. Laws to compel individuals to disclose encryption keys are still relatively new and controversial.

Legal Considerations

The examination of digital media is covered by national and international legislation. For civil investigations, in particular, laws may restrict the abilities of analysts to undertake examinations. Restrictions against network monitoring, or reading of personal communications often exist. During criminal investigation, national laws restrict how much information can be seized. For example, in the United Kingdom seizure of evidence by law enforcement is governed by the PACE act. During its existence early in the field, the "International Organization on Computer Evidence" (IOCE) was one agency that worked to establish compatible international standards for the seizure of evidence.

In the UK the same laws covering computer crime can also affect forensic investigators. The 1990 computer misuse act legislates against unauthorized access to computer material; this is a particular concern for civil investigators who have more limitations than law enforcement.

An individual's right to privacy is one area of digital forensics which is still largely undecided by courts. The US Electronic Communications Privacy Act places limitations on the ability of law enforcement or civil investigators to intercept and access evidence. The act makes a distinction between stored communication (e.g. email archives) and transmitted communication (such as VOIP). The latter, being considered more of a privacy invasion, is harder to obtain a warrant for. The ECPA also affects the ability of companies to investigate

the computers and communications of their employees, an aspect that is still under debate as to the extent to which a company can perform such monitoring.

Article 5 of the European Convention on Human Rights asserts similar privacy limitations to the ECPA and limits the processing and sharing of personal data both within the EU and with external countries. The ability of UK law enforcement to conduct digital forensics investigations is legislated by the Regulation of Investigatory Powers Act.

Digital evidence

When used in a court of law digital evidence falls under the same legal guidelines as other forms of evidence; courts do not usually require more stringent guidelines. In the United States the Federal Rules of Evidence are used to evaluate the admissibility of digital evidence, the United Kingdom PACE and Civil Evidence acts have similar guidelines and many other countries have their own laws. US federal laws restrict seizures to items with only obvious evidential value. This is acknowledged as not always being possible to establish with digital media prior to an examination

Laws dealing with digital evidence are concerned with two issues: integrity and authenticity. Integrity is ensuring that the act of seizing and acquiring digital media does not modify the evidence (either the original or the copy). Authenticity refers to the ability to confirm the integrity of information; for example, that the imaged media matches the original evidence. The ease with which digital media can be modified means that documenting the chain of custody from the crime scene, through analysis and, ultimately, to the court, (a form of audit trail) is important to establish the authenticity of evidence.

Digital investigators, particularly in criminal investigations, have to ensure that conclusions are based upon factual evidence and their own expert knowledge. In the US, for example, Federal Rules of Evidence state that a qualified expert may testify "in the form of an opinion or otherwise" so long as:

(1) The testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

The sub-branches of digital forensics may each have their own specific guidelines for the conduct of investigations and the handling of evidence. In the UK forensic examination of computers in criminal matters is subject to ACPO guidelines. There are also international

approaches to providing guidance on how to handle electronic evidence. The "Electronic Evidence Guide" by the Council of Europe offers a framework for law enforcement and judicial authorities in countries who seek to set up or enhance their own guidelines for the identification and handling of electronic evidence.

Investigative tools

The admissibility of digital evidence relies on the tools used to extract it. In the US, forensic tools are subjected to the Daubert standard, where the judge is responsible for ensuring that the processes and software used were acceptable. In a 2003 paper Brian Carrier argued that the Daubert guidelines required the code of forensic tools to be published and peer reviewed. He concluded that "open source tools may more clearly and comprehensively meet the guideline requirements than would close source tools."

Branches

Digital forensics includes several sub-branches relating to the investigation of various types of devices, media or artefacts.

Mobile device forensics

Mobile device forensics is a sub-branch of digital forensics relating to recovery of digital evidence or data from a mobile device. It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms. Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data. Mobile devices are also useful for providing location information; either from inbuilt gaps/location tracking or via cell site logs, which track the devices within their range.

Network forensics

Network forensics is concerned with the monitoring and analysis of computer network traffic, both local and WAN/internet, for the purposes of information gathering, evidence collection, or intrusion detection. Traffic is usually intercepted at the packet level, and either stored for later analysis or filtered in real-time. Unlike other areas of digital forensics network data is often volatile and rarely logged, making the discipline often reactionary.

Process Models

There have been many attempts to develop a process model but so far none have been universally accepted. Part of the reason for this may be due to the fact that many of the

process models were designed for a specific environment, such as law enforcement, and they therefore could not be readily applied in other environments such as incident response. This is a list of the main models since 2001 in chronological order:

1. The Abstract Digital Forensic Model (Reith, et al., 2002)
2. The Integrated Digital Investigative Process (Carrier & Spafford, 2003)
3. An Extended Model of Cybercrime Investigations (Ciardhuain, 2004)
4. The Enhanced Digital Investigation Process Model (Baryamureeba & Tushabe, 2004)
5. The Digital Crime Scene Analysis Model (Rogers, 2004)
6. A Hierarchical, Objectives-Based Framework for the Digital Investigations Process (Beebe & Clark, 2004)
7. Framework for a Digital Investigation (Kohn, et al., 2006)
8. The Four Step Forensic Process (Kent, et al., 2006)
9. FORZA - Digital forensics investigation framework (Ion, 2006)
10. Process Flows for Cyber Forensics Training and Operations (Venter, 2006)
11. The Common Process Model (Freiling & Schwittay, (2007)
12. The Two-Dimensional Evidence Reliability Amplification Process Model (Chair, et al., 2008)
13. The Digital Forensic Investigations Framework (Selma, et al., 2008)
14. The Systematic Digital Forensic Investigation Model (SRDFIM) (Agarwal, et al., 2011)

Seizure

Prior to the actual examination digital media will be seized. In criminal cases this will often be performed by law enforcement personnel trained as technicians to ensure the preservation of evidence. In civil matters it will usually be a company officer, often untrained. Various laws cover the seizure of material. In criminal matters law related to search warrants is applicable. In civil proceedings the assumption is that a company is able to investigate their own equipment without a warrant, so long as the privacy and human rights of employees are observed.

Acquisition

Once exhibits have been seized an exact sector level duplicate (or "forensic duplicate") of the media is created, usually via a write blocking device, a process referred to as Imaging or Acquisition. The duplicate is created using a hard-drive duplicator or software imaging tools such as DCFLdd, IXimager, Guymager, TrueBack, EnCase, FTK Imager or FDAS. The original drive is then returned to secure storage to prevent tampering.

The acquired image is verified by using the SHA-1 or MD5 hash functions. At critical points throughout the analysis, the media is verified again, known as "hashing", to ensure that the evidence is still in its original state.

Analysis

After acquisition the contents of (the HDD) image files are analyzed to identify evidence that either supports or contradicts a hypothesis or for signs of tampering (to hide data). During the analysis an investigator usually recovers evidence material using a number of different methodologies (and tools), often beginning with recovery of deleted material. Examiners use specialist tools (EnCase, ILOOKIX, FTK, etc.) to aid with viewing and recovering data. The type of data recovered varies depending on the investigation; but examples include email, chat logs, images, internet history or documents. The data can be recovered from accessible disk space, deleted (unallocated) space or from within operating system cache files.

Various types of techniques are used to recover evidence, usually involving some form of keyword searching within the acquired image file; either to identify matches to relevant phrases or to parse out known file types. Certain files (such as graphic images) have a specific set of bytes which identify the start and end of a file, if identified a deleted file can be reconstructed. Many forensic tools use hash signatures to identify notable files or to exclude known (benign) ones; acquired data is hashed and compared to pre-compiled lists such as the Reference Data Set (RDS) from the National Software Reference Library

On most media types including standard magnetic hard disks, once data has been securely deleted it can never be recovered. SSD Drives are specifically of interest from a forensics viewpoint, because even after a secure-erase operation some of the data that was intended to be secure-erased persists on the drive.

Once evidence is recovered the information is analyzed to reconstruct events or actions and to reach conclusions, work that can often be performed by less specialist staff. Digital investigators, particularly in criminal investigations, have to ensure that conclusions are based upon data and their own expert knowledge. In the US, for example, Federal Rules of

Evidence state that a qualified expert may testify “in the form of an opinion or otherwise” so long as:

(1) The testimony is based upon sufficient facts or data,

(2) The testimony is the product of reliable principles and methods, and

(3) The witness has applied the principles and methods reliably to the facts of the case.

Reporting

When an investigation is completed the information is often reported in a form suitable for non-technical individuals. Reports may also include audit information and other meta-documentation.

When completed reports are usually passed to those commissioning the investigation, such as law enforcement (for criminal cases) or the employing company (in civil cases), who will then decide whether to use the evidence in court. Generally, for a criminal court, the report package will consist of a written expert conclusion of the evidence as well as the evidence itself (often presented on digital media).

Software of digital Forensics

1. Digital Intelligence Software
2. Access data
3. Guidance Software
4. Paraben Forensic Tools
5. Pass ware
6. Belk soft
7. Susteen
8. Hot Pepper Technology

20. EXPERT OPINION AND REPORT WRITING

Documenting an investigation is as important as performing it. A poorly documented case file can lead to a disappointing conclusion, can result in a dissatisfied client, and can even

damage the financial accounting investigator's reputation and that of the investigator's firm. Various means by which the Forensic Investigator may report his findings are discussed in greater detail in this chapter.

Depending on the professional affiliations, one will be required to follow the reporting standards of their profession.

TYPES OF REPORTS

The following types of reports are relevant.

Written reports

Report of investigation. This form of written report is given directly to the client, which may be the company's management, board, audit committee of the board, in-house counsel or outside counsel. The report should stand on its own; that is, it should identify all of the relevant evidence that was used in concluding on the allegations under investigation. This is important because the client may rely on the report for various purposes such as corporate filings, lawsuits, employment actions, or alterations to procedures and controls.

Expert report filed in civil court proceedings

Affidavits. These are voluntary declarations of facts and are communicated in written form and sworn to by the witness (declarant) before an officer authorized by the court.

Informal reports. These consist of memos to file, summary outlines used in delivery of an oral report, interview notes, spreadsheets listing transactions along with explanatory annotations, and other, less-formal written material prepared by the investigation team.

Oral reports

Oral reports are usually given by the forensic investigation engagement leader to those overseeing an investigation, such as a company's board, or to those who represent the company's interests, such as outside counsel.

Oral reports involve giving a deposition—as a fact witness or expert witness—during which everything that is said, by all parties to the deposition is transcribed by a court reporter.

BASIC ELEMENTS TO CONSIDER FOR INCLUSION IN A REPORT

- Identify your client
- In the case of a lawsuit, identify the parties

- State in broad terms what you were asked to do
- Describe your scope, including the time period examined
- Include mention of any restriction as to distribution and use of the report
- Identify the professional standards under which the work was conducted
- Identify exclusions in the reliance on your report
- State that your work should not be relied on to detect fraud
- Include the procedures you performed, technical pronouncements relied upon, and findings
- Conclusions Based on Work Performed
- Summarizing your findings

A summary can be helpful to the reader but may be perilous for the report writer in terms of keeping critical information and perspectives intact. Caution is advised when preparing two types of summary sections: executive summary and conclusion.

It is not recommended to write a summary conclusion. If for any reason one nonetheless does so, one should be careful not to offer an opinion on the factual findings

WORKING PAPERS

A forensic investigator, once engaged, needs to take certain internal steps to document procedures, findings, and in some cases, recommendations. These elements of the investigation process are documented in a collection of evidence termed working papers, which divide into two broad categories: internal/administrative and substantive work product.

Depending on the assignment, substantive working papers in either hard copy or electronic form may include many different items.

Any working papers created by the engagement team should be clearly marked to indicate the name of the creator, the date, the source of information, the information's classification, and the issue addressed. Such working papers should also be secured so as to ensure that only members of the immediate engagement team have access to them. Certain matters will require the forensic investigators to prove that they have used reasonable means to secure from others the working papers and other evidence. In such matters, custody can be proved

by ensuring that working papers be kept in a secure room with a sign-in sheet for all who have access to the room.

MISTAKES TO AVOID IN REPORTING

Avoid Overstatement

The closer one sticks to the facts, all the facts, and just the facts, without embellishment, the better the report. The facts should speak for themselves. This is not to say that all facts are created equal: some facts are smoking-gun discoveries—for example, memos demonstrating both knowledge and intent. However, even in respect of obviously important facts, one should be careful not to overstate them.

Use Simple, straight forward language focused on the Facts

The task of the forensic investigator is to take a complex situation, properly investigate it to determine the relevant facts, and then report those facts in a simple, straightforward manner so that the reader or person hearing the report understands the facts and how they should be interpreted for resolution of the allegations. Who was involved? How much damage was caused? How did the events occur? Why did the company not catch the problem earlier? In reporting the answers to these questions, there is no room for speculation.

RELATIONSHIP REVIEW

Most firms that provide Forensic Investigation services have their own procedures for performing a relationship review, or conflicts check, that is, identifying relationships that the firm may have had or now has with any of the parties involved.

The points reviewed and documented may well include the following:

- The date on which the relationship review was cleared
- The individual who cleared it
- Notations of pertinent discussions in clearing current and prior relationships
- The date on which the assignment was accepted

In order for Forensic Investigation to become familiar with a specific company or situation, they may perform some background research such as checking the Internet, performing a public records search, and searching various fee-based data bases. However, no investigative work of substance should begin before the relationship check has cleared. Identifying a conflicting relationship that may preclude a firm from accepting the assignment after work

has begun reflects negatively on the practitioner, the firm, and even the client, especially if court-imposed deadlines—such as deadlines for naming experts—have passed.

20. FORENSIC INVESTIGATION REPORT FORMAT

TO:
FROM:
SUBJECT:
REF:
DATE:

I. Background

The background section should generally be about two paragraphs. It should state very succinctly why the fraud examination was conducted (e.g., an anonymous tip was received, an anomaly was discovered during an audit, money or property was missing).

You may also state who called for the examination and who assembled the examination team.

II. Executive Summary

For a simple fraud examination, the executive summary should be no more than four or five paragraphs. For a more complex case, the summary may reach a page in length. In this section, you should also summarize what actions you performed during the fraud examination, such as reviewing documents, interviewing witnesses, conducting analyses or tests, etc. It provides the reader with an overview of what you did during the examination process. At the end of this section, you should summarize the outcome of the examination.

III. Scope

This section should consist of just one paragraph explaining what the scope of the fraud examination was. For example, “Determine whether or not inventory was misappropriated from the warehouse,” or “Determine why money is missing from the bank account.”]

For Example:

The objective of the Fraud Examination Team was as follows:

Determine the existence of a possible misappropriation of assets of XYZ Ltd, Incorporated. The examination is predicated upon an anonymous telephone call alleging improprieties on the part of Linda Reed Collins, Bailey's purchasing manager.

IV. Audit Approach

This section gives a brief description of the following items:

a) Fraud examination team members

b) Procedures (generally what documents were reviewed or what tests were conducted)

c) Individuals interviewed It provides a handy reference as to who was involved in the fraud examination, what the team reviewed, what tests or analyses were conducted, and what individuals the team interviewed.

V. Audit Findings

This section contains the details of the fraud examination. It will generally consist of several pages. In this section you should describe what tasks you performed and what you found. Provide enough detail so that the reader understands what occurred, but not so much detail that the reader begins to lose interest or becomes bogged down in the details. The reader wants to know how many invoices were forged, who was involved, how did they do it, what proof do you have, etc. If the findings section is long, you may wish to use subheadings for particular topics or individuals to make it easier for the reader to stay organized. The information can be presented either chronologically or by topic — whatever makes it easier for the reader to follow.

VI. Summary

This section should be one or two paragraphs and should succinctly summarize the results of the fraud examination. It should be similar to the outcome stated at the end of the Executive Summary section.

VII. Disclaimer

In this section auditor should write report disclaimer and limitations to the assignment if any to safeguard himself on accuracy of the data or information gathered including audit evidence and/or provided by the client.

21. FORMATS FOR VARIOUS UNDERTAKINGS/CERTIFICATES

CONSENT TO RECORD

_____ (Date)

_____ (Location)

I, _____ (Name)

_____

_____ (Address), hereby authorize _____and_____ _____,

Representative of_____(Company Name), to place a Body Recorder on my person for the purpose of recording any conversation with_____ _____(Name of subject (s)) which I might have on or_____(Date)

I have given this permission voluntarily and without threats or promises of any kind.

_____

(Signature)

Witness:

1._____

2_____

CONSENT TO SEARCH

_____ (Date)

_____ (Location)

I, _____ (Name), having been informed of my constitutional right not to have a search made of the premises hereinafter mentioned without a search warrant and of my right to refuse to consent to such a search,

hereby authorize _____ _____, and _____ to conduct a complete search of my premise located at_____. The above-mentioned individuals are authorized by me to take from my premises any letter, papers, materials or other property which they might desire.

This written permission is being given by me voluntarily and without threat or promises of any kind.

_____

(Signature)

Witnesses:

1._____

2._____

This is to certify that on _____at_____ _____, the individual described above, conducted a search of _____ _____.

I certify that nothing was removed from my custody.

_____

(Signature)

Witnessed:

1._____

2._____

CONSENT TO SEARCH

On (date) _____item (s) listed below were:

_____Received from

_____Returned to

_____Released to

(Name)_____

_____

(Street Address)

_____

(City)_____

_____

Description of item (s):

1. _____

_____

2. _____

_____

3. _____

_____

4. _____

_____

5. _____

_____

6. _____

_____

7. _____

_____

8.

_____

_____

Received by:

_____

Received from:

_____

CUSTOMER CONSENT AND AUTHORIZATION FOR ACCESS TO FINANCIAL RECORDS

I, _____ (Name of customer), having read the explanation of my rights which is attached to this form, hereby authorize the _____

_____ (Name and address of Financial Institution) to disclose these financial records:

To, _____ (Name of person (s))

For the following purpose (s):

_____

_____

I understand that this authorization can be revoked by me in writing at any time before my records, as described above, are disclosed, and that this authorization is valid for not more than three months from the date of my signature.

_____ (Date) _____

(Signature of Customer)

_____

(Address of Customer)

_____

(Witness)

EVIDENCE CONTROL LOGS

Bank Safe Deposit Box: _____ (Name of Bank)

Evidence control centre location_____ _____ (Address of Bank)

REPOSITORY

Office safe/ Vault Location_____ others: _____ (Files Cabinet, etc.)

Location: _____

(1) Signature of person(s), placing evidence in or removing from repository. If entry to facility for other reasons, briefly state in cola 2.	(2) Reasons	(3) File case No.	Entered		Departed	
			Time	Date	Time	Date

APPENDIX A

FRAUD EXAMINATION CHECKLIST

Case Name: _____ Case No.: _____

Synod.	Particulars	Yes	No
1.	Fully debriefed all informants and Witnesses?		
2.	Documented the allegation in writing?		
3.	Identified all possible Schemes or indicators of fraud?		
4.	Developed Fraud Theory?		
5.	Notified legal counsel and discussed whether to proceed?		
6.	Obtained, Recorded and filed all pertinent information and documents in the files?		
7.	Determined the potential loss?		
8.	Identified potential witnesses?		
9.	Determined if error or mistake made?		
10.	Reviewed Internal controls?		
11.	Developed an investigative plan?		
12.	Determined the type of evidence needed to pursue?		
13.	Identified indicators showing intent?		
14.	Reviewed payroll records and cancelled cheques? – Identified all bank accounts – Identified number of exemptions – Identified who might be endorsing cheques		

Synod.	Particulars	Yes	No
15.	Reviewed personal expense reports? – Identified unusually high expenses – Identified credit card used – Identified where suspect entertains clients – Identified duplicate submissions		
16.	Performed background/ asset check? – Driver's license violations – Motor vehicle registration records – Regulatory licenses – Vital statistics – Building permits		
	– Business filings • Fictitious names Indices • Business licenses • Corporate records • Limited partnerships • SEC filings – Country and State records • Criminal • Civil • Domestic • Probate • Real estate records – Federal court filings		

Synod.	Particulars	Yes	No
	• Criminal • Civil • Bankruptcy – Consumer credit records – Business reporting services		
17.	Determined who should be interviewed?		
18.	Developed interview approach?		
19.	Preformed Financial Analysis – Vertical Analysis – Horizontal Analysis – Ratio Analysis – Rationalizations – Industry Analysis – Net Worth Analysis		
20.	Will undercover operation be used? – Plan developed – Approval received – Operation completed		
21.	Will Surveillance be used? – Plan developed – Personnel set up – Surveillance curtailed		

Synod.	Particulars	Yes	No
22.	Developed other informants?		
23.	Use Mail covers?		
24.	Performed link Analysis?		
25.	Identified computers that might be linked to investigation? – Identify expertise needed – Data downloaded – Data printed		
26.	Performed Forensic Analysis – Handwriting – Typewriter – Reviewed altered documents – Ink analysis – Document restoration		
27.	Interview conducted? – Interview documented – Signed statements received		
	– Identified other witnesses to interview – Interviewee knows how to get in touch with one		
28.	Completed documentation and report to management?		
29.	Notified Management?		
30.	Employee(s) terminated?		

Synod.	Particulars	Yes	No
	– Received identification badge or deleted from system – Notified security not to allow access to corporate premises – Personal belongings identified and arrangements made for employee to collect		
31.	Report written? – Heading – Summary – Memorandum – Pertinent correspondence – Documentation of interviews – Pertinent evidence included – Index – Cover page – Report approved by supervisor		
32.	Appointment made with law enforcement agency?		
33.	Follow-up contract made with investigators?		

APPENDIX A

FRAUD EXAMINATION CHECKLIST

Case Name: _____ Case No.: _____

S. No.	Documents to be Examined	To Do	Date Received

S. No.	Documents to be Examined	To Do	Date Received
1.	ACCOUNTING RECORDS: • Balance Sheet • Income Statement • Statement of cash flows • Bank statement • Expense account • Computer password • others		
2.	PERSONNEL RECORDS: • Date of Employment • Signed ethics agreement (conflict of interest statement) • Current address • Prior address • Spouse's Name • Maiden Name • Children's Name • Prior Employment • Prior supervisor • Insurance information (covered dependents) • Employee evaluation (performance reviews) • Garnishments • Vacation schedule		

S. No.	Documents to be Examined	To Do	Date Received
	• Other		
3.	PERSONAL RECORDS • Bank statements • Tax returns • Insurance policies • Mortgage records • Brokerage statements • Credit card statements • Telephone records • Other business records • Investments • Vehicle information • Diaries (calendars)		
4.	PUBLIC RECORDS PERSONAL • Civil filing: State Federal • Criminal Filings: State Federal • Property Tax Records: By Name By Address Tax Liens Financing		

S. No.	Documents to be Examined	To Do	Date Received
	Other • Judgments: Garnishments • Domestic Relations Records Divorce Property statement Financial Statement		
	Tax Returns Depositions Probate Records • U.S. Bankruptcy Filings: Financial Statements Bank Statements Property ownership • Education Verification: University/ College Professional Licenses UCC Filings • Corporate Records: Company Name Individual (Incorporators) Assumed Name Index • Vehicle owned: Lien holder • Boats Owned: Lien holder • Aircraft Owned: Lien holder		
5.	PUBLIC RECORDS – BUSINESS – Utility records – UCC Filings		

S. No.	Documents to be Examined	To Do	Date Received
	– Tax Receipts • Tax liens • Who actually pays the taxes? – Post Office Box Application – Civil Filings • State • Federal – Assumed Name Index – Corporate Charter (Bylaws) – Business Credit History • Dun & Bradstreet • Better Business Bureau – others		

APPENDIX A

FRAUD EXAMINATION CHECKLIST

Case Name: _____ Case No.: _____

Adverse Witnesses:

Name	Phone	Date Contacted	Interview Completed	Report Date

22. USEFUL WEBSITES

Sr. No.	Description	Website
1	Association of Certified Fraud Examiners	http://www.acfe.com/
2	Serious Fraud Investigation Office, India	http://sfio.nic.in/websitenew/main2.asp
3	The Central Bureau of Investigation	http://cbi.nic.in/
4	Enforcement Directorate	www.enforcementdirectorate.gov.in/
5	The Reserve Bank of India	https://www.rbi.org.in/

6	Insurance Regulatory and Development Authority	https://www.irda.gov.in/
7	Financial Intelligence Unit - India (FIU-IND)	http://fiuindia.gov.in/
8	The Securities and Exchange Board of India (SEBI)	www.sebi.com/
9	Financial Intelligence Unit of International Monetary Fund	http://www.imf.org/external/pubs/ft/FIU/
10	Ministry of Corporate Affairs	http://www.mca.gov.in/
11	Supreme Court of India	http://supremecourtofindia.nic.in/
12	Telecom Disputes Settlement and Appellate Tribunal	www.tdsat.nic.in/