HANDBOOK ON FORENSIC ACCOUNTING & FRAUD PREVENTION

Global Forensic Audit & Investigation
(A Division of Meridien Business Consultants Pvt. Ltd)
www.globalforensic.in

PREFACE

Statistics quoted in a recent report by the Association of Certified Fraud Examiners' (ACFE) 2014 titled "Report to the Nation on Occupational Fraud and Abuse" has estimated that a typical organization loses 5% of its revenues to fraud each year and cumulative annual fraud loss globally during 2013 could have been of the order of more than $3.7 trillion. The banking and financial services, government and public administration, and manufacturing industries continue to have the greatest number of cases reported.

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. All these developments have added to the increasing need for a check on these systems which can be in the form of Forensic Auditing.

This Book will give an exhaustive outlook over Forensic Accounting right from the evolution of Forensic Audit to the current scenario. It is a comprehensive compendium on the scope, the processes, the techniques and its advantages etc stated in a very simple manner.

We are confident that this publication **"Handbook on Forensic Accounting & Fraud Prevention"** will be of immense benefit to all readers.

Research Team

Global Forensic Audit & Investigation

CONTENTS

❖ Forensic Accounting

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 realised earlier is entered later on; what is realised later is entered earlier; what ought to be realised is not realised; what is hard to realise is shown as realised; 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) 2014 titled "REPORT TO THE NATION ON OCCUPATIONAL FRAUD AND ABUSE" may have some answers. The report has estimated that a typical organization loses 5% of its revenues to fraud each year and cumulative annual fraud loss globally during 2013 could have been of the order of more than $3.7 trillion. 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 $500,000. Employees, conversely, committed 42% of occupational frauds but only caused a median loss of $75,000. Managers ranked in the middle, committing 36% of frauds with a median loss of $130,000. 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 $80,000, but as the number of perpetrators increased, losses rose dramatically. In cases with two perpetrators the median loss was $200,000, for three perpetrators it was $355,000 and when four or more perpetrators were involved the median loss exceeded $500,000. 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, 58% of the victim organizations had not recovered any of their losses due to fraud, and only 14% 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, blood-splattered implements at the scenes of crime and autopsies and post mortems. Nothing can be further from the truth. Forensic accounting 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 Accounting. It is the study

and interpretation of accounting evidence. It is the application of accounting methods to the tracking and collection of forensic evidence, usually for investigation and prosecution of criminal acts such as embezzlement or fraud. *Forensic Auditing*, for want of a better definition, is therefore a specialised mode of auditing 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 Accounting can sometimes be referred to as Forensic Auditing.

Forensic audit 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 unauthorised 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 accounting would be complete without a passing mention of this specialised field.

Computer forensics is simply the application of computer science to the investigative process. As investigative accounting is an important aspect of forensic accounting, computer forensics and its sub-disciplines are important tools for the forensic accountant 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 enhancement, video and audio enhancements and database visualisation, are tools, techniques and skills which are becoming more critical in the field of forensic accounting 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 type of financial sector frauds (bank fraud) like stolen cheque, cheque kiting, rogue trader, fraudulent loan and applications for loan, and many more.
- `Skiming 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' authorisation 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.

❖ **Forensic Auditor**

Principal Duties of a Forensic Auditor

Simply put, a forensic auditor's primary duty is to analyse, interpret, summarise and present complex financial- and business-related issues in a manner that is both understandable by the layman and properly supported by the evidence.

Forensic auditors are engaged by both government and private agencies cutting across industries ranging from insurance companies, banks, police forces, regulatory agencies and other financial and business organisations.

The services rendered by forensic auditor cover a wide spectrum of which the following are commonly provided:

- investigation and analysis of financial evidence;

- development of computerised applications to assist in the analysis and presentation of financial evidence;
- communication of findings in the form of reports, exhibits and collections of documents; and
- Assistance in legal proceedings, including testifying in court as expert witness and preparing visual aids to support trial evidence.

To properly carry out these functions, the forensic auditor must also be familiar with legal concepts and procedures, including the ability to differentiate between substance and form when grappling with any issue.

Specific Assistance in Investigative Accounting and Litigation Support

The forensic auditor can provide more specific assistance in the following ways.

Investigative accounting

- Reviewing the factual situation and providing suggestions on alternative course of action.
- Assisting in the preservation, protection and recovery of assets.
- Coordinating with other experts, including private investigators, expert document examiners, consulting engineers and other industry specialists.
- Assisting in the tracing and recovery of assets through civil, criminal and other administrative or statutory proceedings.

Litigation support

- Assisting in securing documentation necessary to support or rebut a claim.
- Reviewing relevant documentation to provide a preliminary assessment of the case and identify potential areas of loss and recovery.
- Assisting in the examination and discovery process, including the formulation of relevant questions regarding financial evidence.
- Attending to the examination and discovery process to review the testimony, assisting with understanding the financial issues and formulating additional questions for counsel.
- Reviewing the opposing expert's reports on damages and the strengths and weaknesses of the positions taken.

- Assisting in settlement meetings and negotiations.
- Attending the trial to hear testimony of opposing experts and assisting in the cross-examination process.

❖ Typical Approach to a Forensic Investigation

What does a forensic auditor do when alerted to a fraud and instructed to proceed when appointed? There are usually five areas which the forensic accountant 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 accountant, 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 accountant's team of forensic IT personnel would be indispensable in any investigation.
5. Interview key company employees - formally and informally.

❖ Difference between Forensic Audit 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 auditors and those of financial auditors

Sr.no.	Particulars	Other Audits	Forensic Audit
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.

ADVANTAGES OF FORENSIC AUDIT

Forensic audit 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 Auditor?

A logical question to pose is why bring in a forensic auditor 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 Auditing:

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

4. **Arbitration service:** Forensic accountants 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 accountants to have an accurate assessment of claims to be settled.
   Similarly, policyholders seek the help of a forensic accountant when they need to challenge the claim settlement as worked out by the insurance companies. A forensic accountant handles the claims relating to consequential loss policy, property loss due to various risks, fidelity insurance and other types of insurance claims.

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

Key Benefits of Using Forensic Auditors

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 accountants 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 accountant 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 accountant 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 arises 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.

EVOLUTION OF FORENSIC AUDIT IN THE WORLD

Though Forensic Auditing 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 Accounting 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 Accountants 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 accounting 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 accounting is gaining importance.

Today's forensic accountants are involved in a wide variety of cases, from the more mundane family law and commercial matters through to a range of criminal investigations, which include white-collar crimes such as business and insurance fraud through to organised crime, murder and even terrorism where forensic accountants 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 Accountants. 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 Accountant with them for their expertise. Forensic Accountants 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 Accountants 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 whistleblowers to come forward. If a whistleblower 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 Accountants to be involved.

Forensic Accounting has taken many great leaps of growth in recent history. The Accounting industry has gradually called for more and more Forensic Accountants. It is predicted that growth of the industry, based on the amount of jobs, will reach 6.7% for the years between 2013 and 2018.

EVOLUTION OF FORENSIC AUDIT 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 accounting in India has come to limelight only recently due to rapid increase in Frauds and the white collar crimes and the belief that our law enforcement agencies do not have sufficient expertise or the time needed to uncover frauds. 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 accounting, irrespective of whether we understand the need or not.

In India, Forensic Accounting 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 task of Forensic Accountants is handled by Chartered Accountants who apart from handling traditional practice of auditing as required under the Companies Act, 1956 or Income Tax Act are called upon by the law enforcement agencies or the companies or private individuals to assist in investigating the financial crime or scam.

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 accountants.

There is no mention of Forensic accountants in the Indian statutes so far but there are various provisions related to Forensic accountants/auditors in the statutes. The introduction of the Companies Act, 2013 has a significant impact on fighting and preventing frauds. Under section 245 (1g) of the new Companies Act, depositors and members of a company can claim damages from auditors, management and other consultants for the wrongdoings by the company and its management. Many consultants and senior executives are expected to become part of the certified community. Further, under section 140 the auditors and their firm would be jointly liable for any

frauds in the books of accounts and many auditors are likely to become forensic accountants in the days to come to avoid being caught on the wrong foot. Under section 149(12), independent directors would be held liable for the frauds in their knowledge.

STEPS / CONDUCT OF FORENSIC AUDIT – PROCEDURES

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 accounting 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 accounting 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 accounting procedures. Instead, all relevant evidence is sought and examined. Based on the investigative findings, the forensic accounting 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 accounting investigator takes preventive actions to eliminate recurrence of the problem. The forensic accounting investigator's findings and recommendations may form the basis of testimony in litigation proceedings or criminal actions against the perpetrators.

Broad Stages of Forensic Audit:

1. Accepting the investigation
2. Planning

3. Evidence Gathering
4. Reporting
5. Court Proceedings

1. **Accepting the investigation:**
    - Forensic Auditors must ensure whether their firm has necessary skills and experience to accept the work.
    - Ideally statutory Auditors should not accept forensic auditing 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 Accountants do not testify that fraud has occurred but only present evidence.

PREVENTION OF FRAUDS & RISK MITIGATION

Fraud and white collar crime have increased considerably over the last ten years, 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 show the astronomical values associated with fraud. Also, the expansion of computers into businesses may make organizations more vulnerable to fraud and abuse.

In order to combat fraud and white collar crime in businesses, a concerted effort must be exerted by the management of the business, the external auditors, and by all employees of the business. Everyone must realize that fraud is not a victimless crime. The cost of fraud and theft are shared by all through higher costs and lower corporate profits. Through adequate internal controls by management, better working environments for employees, more stringent requirements for external auditors, and codes of ethics for employees, everyone can start to combat frauds and defalcations within corporate

1. **Set clear standards.** One of the best ways to help safeguard a business is to set clear standards from the beginning. This includes an appropriate example and ethical tone, starting from the top down. An employee manual can be helpful in establishing the principles and values to guide your organization. In a small organization, an employee manual levels the playing field and keeps the rules from becoming arbitrary. The rules apply to everyone. If someone is dismissed and you find yourself in court, the manual can be a reference that explains what actions warrant dismissal.

2. **Check employee references.** When hiring new employees check references and perform background checks that include employment, credit, licensing and criminal history. The cost is far outweighed by the benefit. For example, a business owner should be wary of hiring a bookkeeper with bad credit because the weight of crippling financial obligations could turn an otherwise honest person into a thief.

3. **Secure your organization.** Some deterrents are simple to initiate, but often go ignored. Secure organizations, for example, closely guard and monitor their checks. Using pre-numbered checks enables you to audit for missing checks. Also, checks clearing out of

sequence can be spotted more easily. All checks should be kept under lock and key, and keys should not be distributed. Other precautions include having a "voided check" procedure and never signing blank checks. All disbursements should be reviewed on a regular basis. Scan then scrutinize checks made out to suppliers you don't recognize, checks made out to an amount for cash, and missing check numbers or checks appearing out of sequence.

4. **Safeguard payroll.** Payroll is another area subject to abuse. Small-business owners and managers should take the extra time to review every payroll check personally. Although time consuming, this procedure provides a monitor to assure employees are being paid appropriately. This can be especially important when a business has temporary and part-time staff. Although not always possible in a small business, certain duties should be maintained separately. For instance, the person who "cuts" or has custody of the checks should never be the person who has authority to sign. The person opening the mail should not record the receivables and reconcile the accounts. Even a small business can take some steps to separate important functions.

5. **Control who reviews sensitive documents.** Small-business owners should control who first receives the bank statements and other sensitive documents. It is not farfetched for a small-business owner to have a separate post office box for the purpose of receiving bank statements, customer receipts or any other sensitive documents. This helps eliminate the possibility that someone intercepts the mail first for the purpose of stealing or covering up an earlier theft.

6. **Consider independent review.** All account reconciliations and general ledger balances should have an independent review by a person removed from the day-to-day transactions, because theft often occurs when bookkeeping is sloppy and unsupervised. People outside the direct bookkeeping function within your organization should be familiar with your company's bookkeeping and record system. This permits spot checks and reviews, better ensuring nothing is amiss and providing a deterrent for fraudulent activities.

7. **Consider hiring a Professional.** If a business owner is not in a position to provide this level of review, make sure your client knows that Professional can be hired to take on some of the independent review function, or provide all of the required bookkeeping services. Make sure you are clear that a Professional providing these services will not necessarily uncover fraud, but will enhance the control environment, possibly deterring fraudulent activities and benefiting the business owner on many different levels. For example, Professional can review monthly financial results with the owner, helping to spot trends indicative of fraud or to find opportunities to enhance profitability.

8. **Consider annual audits.** Even though it may not be required, obtaining an annual audit is a good idea. An audit will not discover all fraud within an organization, but it will give you an opportunity for someone removed from the daily operations to take a "bird's eye view" of the business. An audit also tends to motivate all bookkeeping-related staff to keep things honest because they can never be sure what questions an auditor is going to ask or what documents an auditor may request to review.

9. **Managerial Controls.** Organizations with one hundred or fewer employees have the greatest median losses per capita. The primary reason for this is because internal controls are less sophisticated and stringent in smaller organizations. So what, if any, are management's responsibilities when it comes to the prevention or detection of fraud? Annual reports of management clearly state that management is responsible for the preparation and integrity of the financial information presented, and the company and management maintain a system of internal controls to provide for administrative and accounting controls. All professional literature makes it clear that the responsibility of internal controls, proper reporting, and the adoption of sound accounting policies rests solely with management, not the auditors.

   To combat the problem of fraud, a crucial element in deterring theft is strict internal controls, segregation of duties, and separation of functions. For example, simple procedures such as not letting the person writing the checks reconcile the bank statement, not letting the receiving department maintain physical inventory records, not letting the person initiating the purchase order approve the payment, and not letting the person maintaining the personnel database also issue payroll checks, may help separate

incompatible functions within a business. Thus, internal controls may be strengthened and fraud deterred by separation of functions.

IMPORTANCE OF INTERNAL CONTROLS

There are several keys to effective fraud prevention, but some of the most important tools in the corporate toolbox are strong internal controls. Equally important, though, are the company's attitude towards fraud, internal controls and an ethical organizational culture. While ethical culture is driven by senior management's control environment ("tone at the top"), buy in from the company's Board of Directors and Audit Committee are also essential in promoting an ethical and transparent environment.

Internal controls should not be thought of as "static." They are a dynamic and fluid set of tools which evolve over time as the business, technology and fraud environment changes in response to competition, industry practices, legislation, regulation and current economic conditions.

While no company, even with the strongest internal controls, is immune from fraud, strengthening internal control policies, processes and procedures definitely makes companies a less attractive target to both internal and external criminals seeking to exploit internal control weaknesses.

Strengthening internal controls is seldom accomplished by enhancing one process; rather it involves a comprehensive review of the risks faced, the existing internal controls already in place and their adequacy in preventing fraud from occurring. An internal control review may be conducted corporate-wide or on a location by location basis, or broken down to the individual business unit level. Generally, a review of this nature involves an in depth examination of people, processes and technology. However, there are other intangibles your organization can not afford to overlook.

Audit Interaction

The first part of strengthening internal controls involves changing the attitude some employees have towards auditors. While it is easy to view auditors as the police department's "Internal Affairs" group--whose sole responsibility it is to ferret out wrongdoing--identifying employees who are breaking the rules, personal and professional success is to be had by viewing auditors as key partners and allies in the battle against fraud. This is further reinforced as the auditor's role

ensures that he or she is always at the forefront of corporate policies, practices, procedures, technology, new products and services, making auditors a valuable source of corporate information.

Communication

One way to strengthen internal controls is by improving the communication process. I've seen countless situations where key stakeholders are unaware of major events occurring within a corporation or business unit. This is problematic as there is no opportunity for management to fix something that they're unaware is broken. Regular interaction and communication between departments is paramount in this process.

Communication protocols must be established and agreed upon enterprise wide. Critical incident event distribution notification processes and procedures must be in place to ensure everyone is aware of an incident and understands what their defined roles are when the incident occurs.

Part of incident awareness lies with the ethics, hotline and event notification systems being used by the corporation pursuant to Sarbanes Oxley requirements. Many industry professionals have experience with the operation of ethics and compliance hotline systems but not all incidents are reported through these compliance mechanisms. One of the key questions surrounds how companies notify key stake holders when an event occurs outside the ethics or compliance system? While this communication often falls under a first responder type program, it is imperative that companies have defined processes and communication protocols in place to notify the key management employees who "need to know."

Segregation of Duties

One area where many companies can significantly strengthen their internal controls involves segregation of duty policies and this is often considered the "primary internal control." It is imperative that there are adequate segregation of duties involving custody, authorization and control of source documents and records. E.g. one person should not have the sole authority to initiate a transaction, authorize or approve a transaction and complete the transaction without appropriate sign off processes and differing levels of management approval. The lack of proper segregation of duty policies is most often the root cause of many fraud and theft events in companies without strong internal controls in this area.

There have been so many examples of fraud committed directly as a result of a company's failure to segregate duties that it's not necessary to focus solely on one. Rather, it's important to examine the common themes which contribute to these frauds. Generally, the fraud usually occurs in a finance area; involves someone with unsupervised control over company funds and documents (checks) and access to banking accounts for deposits and withdraws; there is no segregation of duties and the fraud occurs in companies with lax internal controls. So, for example a bookkeeper is able to write a check to himself without worrying about being detected.

Using established fraud prevention best practices, financial duties (cash disbursements) should always be segregated amongst multiple employees. This usually means that there are multiple employees involved in the financial process with oversight at several places in the process. This ensures that one employee cannot manipulate the entire process and increases awareness amongst employees that someone is not only looking, but conducting random audits to reconcile financial transactions. Check stock should be controlled and secured, secondary levels of management approval and dual signatures on checks and payment authorization on amounts over pre-established financial levels should be required. Further, all employee should have individual financial transactional levels established which vary according to their management levels, or position of authority, business unit needs and ability to obligate the business to a financial commitment.

Lessons Learned

While no company wants to experience internal or external fraud events, victimization may have long term corporate anti-fraud benefits if all departments have comprehensive incident handling protocols and the incident is handled appropriately after the fact.

Appropriate handling always includes post event analysis which provides the company with an excellent "lessons learned" opportunity. During this process stakeholders need to be asking the tough questions and gathering information to identify the factors that allowed the event to occur.

The process should not be viewed as a fault finding mission but a determination of whether there was a company, policy, procedure or guideline in place to address this situation, whether the guidelines were followed as designed or adequate to address (or prevent) the specific situation that occurred.

Technology

While technology enables us to perform essential business functions, there are direct correlations between technology, fraud events and the internal control process. Technological applications are probably the single greatest sources of risk and exposure that businesses face. Robust internal controls, including platform and network access controls, remote usage and password protection policies, are needed to regulate the entire computing platform.

Additionally, there must be internal controls in place for all mobile computing applications and company telecommunication devices like personal computers and smart phones. Given how quickly technology is changing, strengthening internal controls in this area revolves around fluid processes as the technology is not static.

A great example of the evolving technology, risk and demand for internal controls involves cloud computing. While cloud computing is viewed as a way to reduce computing costs, the need for strengthened internal controls is significant as your company's information is not under your direct oversight and control.

Fraud Risk Assessments

In accordance with current legislation and regulation, many of the internal controls in place today are specifically designed to protect Personally Identifier Information (PII), and consumer data in the possession of businesses. In today's business environment, consumer and information protection are paramount. Internal controls can be strengthened through departmental fraud risk assessments, audits, and an examination of policies and procedures, particularly those that involve employees who have direct interaction with consumers and their PII. The methods in which data is gathered, handled, stored, and destroyed in conjunction with the company's data retention practices should be examined in detail. Additionally, an assessment of the information and physical security practices, protection methods and controls surrounding the consumers and their PII data should be conducted to find the vulnerabilities and take corrective actions surrounding these internal controls.

Providing self assessment check lists to department managers and requiring a semi- annual review of policies, practices and procedures is an effective method for assessing key controls and

ensuring that they are adequate for preventing fraud. Additionally, fraud risk assessments safeguard company assets, protecting the company from added liability and financial exposure. Oversight for semi annual review usually comes from either the compliance or audit departments. While PII is a major concern for privacy reasons and data breaches, there are a variety of critical business processes and procedures that could be examined in fraud risk assessments depending on the type of business, the industry and the regulation or oversight of the business. Oversight for fraud risk assessments is typically the responsibility of the company's audit department.

Testing Key Controls

It is essential to differentiate fraud risk assessments from control testing. The primary purpose of fraud risk assessments is gathering information about processes, procedures and controls while control testing determines whether the controls are working as intended or not.

It is important that we test internal controls in a controlled environment as internal controls which are only tested under "live fire," real time conditions may not actually be effective controls at all. Testing is an integral part in any control environment and may be a key indicator in not only assessing how strong the internal controls are but whether they need to be strengthened. Simulated, situational testing may also assess event readiness and effective business unit processes. The type of testing, the regularity of the testing and the testing schedule will vary from business to business and may be determined by individual company needs and regulatory requirements.

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

METHODS OF FRAUD DETECTION

There are two main methods used in the literature to detect fraud: supervised and unsupervised.

1. Supervised

2. Unsupervised

Supervised Method

The most frequently used research methodology is classification (or supervised) methods. Supervised methods utilize prior information (also called labeled information) that contains both legitimate and fraudulent transactions, while unsupervised methods do not require any labeled data. Under the supervised method, a database of known fraudulent or legitimate cases is used to construct models used to detect fraud (Bolton and Hand 2002). The models are trained by prior labeled data, and then fraudulent and legitimate transactions are discriminated in accordance with those models. These methods assume that the pattern of fraud in the future will be the same as that in the past. Neural network models which use the supervised method appear frequently in recent research (Bolton and Hand 2002; Kou et al. 2004; Phua et al. 2005).

A major concern in fraud prevention/detection research is that models may work only for the data that is used in creating the models. The generalize ability of fraud profiles is highly dependent on the context of the original model development and on the target environment. For example, if new data comes into the dataset, those models may not work due to either over-fitting to the training dataset or unknown fraud types. In addition, the robustness of models is a major concern during extension, re-utilization, and adaptation. Considering that fraud perpetrators adapt to find loopholes in an enterprise's current fraud prevention/detection system, this can be a critical weakness. In order to adapt to unknown types of

attacks, it is important that the systems should be dynamically extendable and adjustable. Last but not least, the supervised methods suffer from uneven class sizes of legitimate and fraudulent observations. Generally, the number of fraudulent observations is greatly outnumbered by that of legitimate ones. About 0.08% of annual observations are fraudulent (Hassibi 2000). In other words, even if a model classifies all fraudulent transactions as legitimate regardless of their true identities, the error rate (the number of correctly classified transactions/the total number of transactions) of the model is extremely small, which can be misleading.

Unsupervised Methods:

Unsupervised methods have received far less attention in literature than supervised methods. Unsupervised methods focus on detection of changes in behavior or unusual transactions (i.e. outliers) by using data-mining methods. Anomaly/outlier detection is the recognition of patterns in data that do not conform to expected behavior (Chandola et al. 2009). The major advantage of unsupervised methods is that they do not require labeled information, which is generally unavailable due to censorship (Bolton and Hand 2002; Kou et al. 2004; Phua et al. 2005). The results are not disclosed in public either to maintain an enterprise's competitive advantage or because of public benefits (Little et al. 2002).

Unsupervised methods usually employ suspicion scoring systems that estimate the degree of departure from the norm by utilizing if-then type of outlier rules. Rule-based systems are increasingly used to represent experiential knowledge. The criteria to determine whether a transaction is an outlier may change for various reasons such as cost and efficiency. Decision making by if-then rules is similar to a human's cognitive decision processes, which enables internal auditors to understand and adjust the models if necessary. However, verification/ evaluation of the newly devised models is often difficult, if not impossible, due to lack of testable data. To tackle this weakness, methods such as peer group analysis, where groups with similar profiles are compared, and break point analysis, where recent transactions are compared with past patterns, can be used (Bolton and Hand 2001).

The results of unsupervised methods are not direct evidence that flagged transactions are fraudulent. Instead, the aim of unsupervised methods is to inform that flagged transactions are more anomalous, tending toward either error or fraud, based on the experience, analysis, and preconceptions of the analysts. In other words, a flagged transaction can be legitimate, error, or fraudulent. This outcome is clearly different from that of supervised methods, where outcomes are either legitimate or fraudulent. As Jans et al. (2009) described, an outlier can occur via mistakes (i.e. unintentional errors). It can be said that unsupervised methods consider broader causes than supervised methods. Furthermore, a transaction will be worthy of further investigation if it is flagged by multiple criteria, since normal transactions are unlikely

to be flagged by many indicators. Analogous to other rule-based systems, the actual examination of selected transactions allows for re-parameterization and improvement of the method. However, the verification of resulting flagged transactions requires internal auditors' direct examination

	Supervised Methods	Unsupervised Methods
Pros	1. Accurate for known fraud types 2. Results: fraudulent or not	1. Easy to apply and update 2. Unknown fraud can be found 3. Observations with both types are not necessary 4. Results: worthy of further investigation/attention
Cons	1. Highly unbalanced class sizes (1 out of 1,200) 2. False negatives 3. May work only for known fraud types 4. Highly dependent on historic data that may not be accurate 5. Lower understandability	1. Less accurate than complex methods in the short term 2. As accurate as complex methods in the long term 3. Requires auditor verification

IT TOOLS FOR FRAUD DETECTION:

Forensic accounting in conducting investigation in this internet era uses many investigation tools. Ranging from data mining software to data analysis and sometime the same tools that used by hackers. Forensic Computing is the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable in a court of law. Here are some of those tools used by forensic accounting-

1. Helix

2. ACL Desktop

3. Ultra Block

4. Advance Hash Calculator

5. Password Kit Forensic

1. Helix: Helix3TM is "an internal tool to provide the ability to acquire forensically sound images of many types of hard drives and partitions on systems running unique setups such as RAID arrays" (Gleason & Fahey, 2006, p 9). There are many products in the world that offer the capabilities that Helix has. However, Helix different from many other software imaging because, Helix developed based on Knoppix (one variant of Linux) which are open source and free.

2. ACL Desktop: Audit Command Language (ACL) is developed by ACL Service Ltd Foundation of ACL concepts and practices (2006, p 2) defines ACL as a tool to read and analyse type of files scattered across numerous database on different platforms. ACL maintains data integrity by read only access to all data that they accessed, that is why the source data is never changed, altered or deleted.

3. Ultra-Block: Ultra-Block is a brand name for forensic write blocker hardware. The purpose of this hardware is to prevent the digital forensic accounting to modify the data that they accessed. It is very important for digital forensic accounting to maintain the data submitted to a court as evidence remain authentic. Therefore when they access and analyse the evidence they have to be very careful not to modify, change or alter the data. Ultra-Block is compatible with all leading software imaging application including Helix, EnCase or other software imaging.

4. Advance Hash Calculator: Maintaining integrity of evidence is one of the most things that should be concerned by forensic accounting. Once the integrity of evidence is questionable, the evidence will lost its power in the court. The worst case, the admission of evidence in the court will be rejected. One method that can be used to maintain integrity data in terms of digital forensic is by using hash value. The common hash value methods are MD5 and SHA-1. These hash value program, are include in forensic software imaging such as Helix and EnCase. However, Advance Hash Calculator offers more than MD5 and SHA-1 method to calculate hash value.

5. Password Kit Forensic: Password Kit Forensic is a tool for evidence discovery solution reports all password-protected items on a computer and gains access to these items using the fastest decryption and password recovery algorithms. Password can recovered many password in all files including difficult and strong type password. Password Kit Forensic includes a Portable

version that runs from a USB drive and finds encrypted files, recovers files and websites passwords without modifying files or settings on the host computer. Password Kit Forensic also able to decrypts Bit Locker and True Crypt of hard disk. Password Kit Forensic is suitable for forensic purpose and maintain the authenticity of evidences.

FORENSIC AUDIT TECHNIQUES

The conventional accounting and auditing with the help of different accounting tools like ratio technique, cash flow technique, a standard statistical tool examination of evidences are all part of forensic auditing. In cases involving significant amounts of data, the present-day forensic auditor has technology available to obtain or source data, sort and analyse data and even quantify and stratify results through computer audit and various other techniques. Some of the techniques involved in Forensic Auditing to examine the frauds are:

1. Testing Defenses

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

2. Trend Analysis

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

3. Digital Forensic Examinations

Every transaction leaves a digital footprint in today's computer-driven society. Close scrutiny of relevant emails, accounting records, phone logs and target hard drives is a requisite facet of any modern forensic audit. Digital investigations can become quite complex and require support from trained digital investigators. However, many open-source digital forensics tools are now available to assist you in this phase of the investigation.

4. Face to Face Interviews

Forensic auditing is akin to detective work, and every good detective desires to look his witnesses and suspects in the eye. Personal interviews with the staff of your target entity yield a better understanding of its operations and of the culture that exists within it. According to John J. Hall of the Journal of Accountancy, critical information can be gleaned from interviews with parties who have knowledge of the events without being directly connected to the fraud.

5. Full Financial Auditing

Detailed financial audits can be complex and most often require the assistance of a qualified forensic accountant. Basic financial audit techniques include bank statement reconciliations, scrutiny of all vendor contracts and payments, review of tax returns and analysis of public filings. Financial forensic audit techniques seek to identify suspicious transactions and trace them back to potential perpetrators.

6. Benford's Law

Benford's Law, named for physicist Frank Benford, who worked on the theory in 1938 is a mathematical tool, and is one of the various ways to determine whether variable under study is a case of unintentional errors (mistakes) or fraud. On detecting any such phenomenon, the variable under study is subjected to a detailed scrutiny. The law states that fabricated figures (as indicator of fraud) possess a different pattern from random figures. The steps of Benford's law are very simple. Once the variable or field of financial importance is decided, the left most digit of variable under study extracted and summarized for entire population. The summarization is done by classifying the first digit field and calculating its observed count percentage. Then Benford's set is applied. A parametric test called the Z-test is carried out to measure the significance of variance between the two populations, i.e. Benford's percentage numbers for first digit and observed percentage of first digit for a particular level of confidence. If the data confirms to the percentage of Benford's law, it means that the data is Benford's set, i.e. there is68% (almost 2/3rd) chance of no error or fraud. The first digit may not always be the only relevant field. Benford has given separate sets for 2nd, 3rd and for last digit as well. It also works for combination numbers, decimal numbers and rounded numbers. There are many advantages of Benford's Law like it is

not affected by scale invariance, and is of help when there is no supporting document to prove the authenticity of the transactions.

Benford's Law holds true for a data set that grows exponentially (e.g., doubles, then doubles again in the same time span), but also appears to hold true for many cases in which an exponential growth pattern is not obvious (e.g., constant growth each month in the number of accounting transactions for a particular cycle). It is best applied to data sets that go across multiple orders of magnitude (e.g., populations of towns or cities, income distributions). While it has been shown to apply in a variety of data sets, not all data sets follow this theory.

The theory does not hold true for data sets in which digits are predisposed to begin with a limited set of digits. For instance, Benford's Law will not hold true for data sets of human heights, human weights and intellectual quotient (IQ) scores. Another example would be small insurance claims (e.g., between US $50 and US $100). The theory also does not hold true when a data set covers only one or two orders of magnitude.

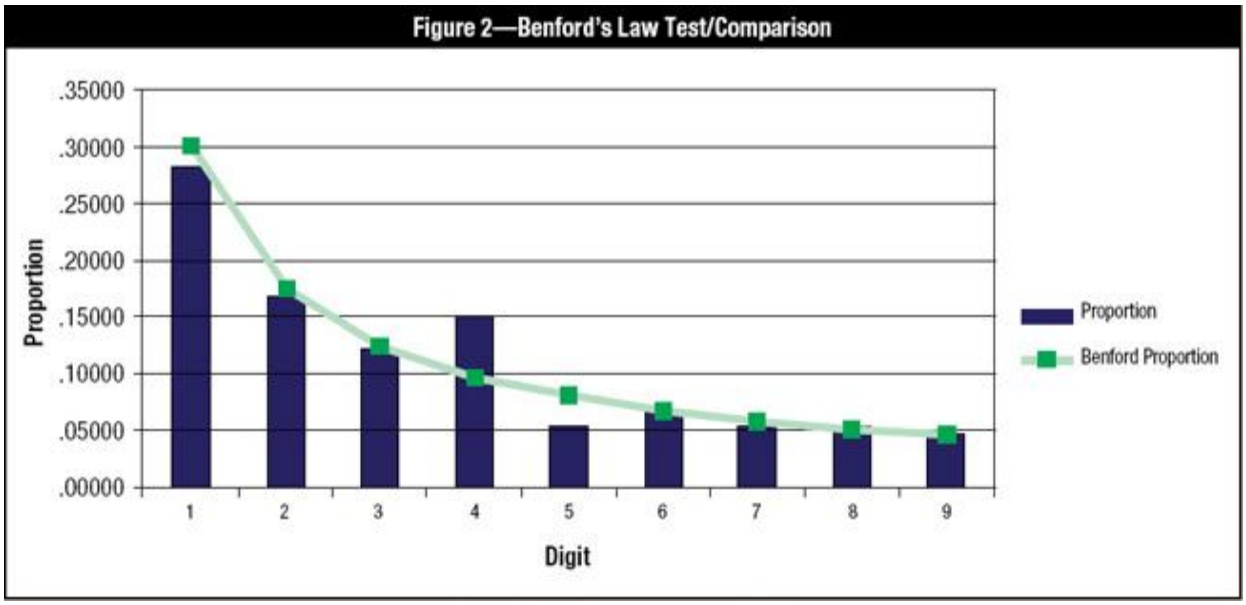
Right Circumstances for Using Benford's Law

Almost from the beginning, proponents of Benford's Law have suggested that it would be a beneficial tool for fraud detection.

A recent example is Mark Nigrini's research, which showed that Benford's Law could be used as an indicator of accounting and expenses fraud. One fraudster wrote numerous checks to himself just below US $100,000 (a policy and procedure threshold), causing digits 7, 8 and 9 to have aberrant percentages of actual occurrence in a Benford's Law analysis. Digital analysis using Benford's Law was also used as evidence of voter fraud in the 2009 Iranian election. In fact, Benford's Law is legally admissible as evidence in the US in criminal cases at the federal, state and local levels. This fact alone substantiates the potential usefulness of using Benford's Law.

Of course the usage of Benford's Law needs to "fit" the audit objective. Some uses are fairly easy to determine for fit. For instance, if the audit objective is to detect fraud in the disbursements cycle, the IT auditor could use Benford's Law to measure the actual occurrence of leading digits in disbursements compared to the digits' probability. Some good examples include thresholds and cutoffs.

For instance, if a bank's policy is to refer loans at or above US $50,000 to a loan committee, looking just below that approval threshold gives a loan officer the potential to discover loan frauds. If loan fraud was being perpetrated, a Benford's Law test of looking at either the leading digit (specifically, the 4) or two leading digits (specifically, 49) has the potential to uncover the fraud. **Figure 2** shows what a Benford's Law test of the leading digit might show as a result in this particular scenario. The line is Benford's Law probabilities and the bars are the actual occurrences. Note that 4 is aberrantly high in occurrence, and 5 is too low, indicating the possible manipulation of the natural occurrence of loans beginning with 5 (US $50,000 loans) possibly being switched to just under the cutoff or indicating that the suspect could be issuing a lot of $49,999.99 loans fictitiously to embezzle funds.



Another example might be a cutoff of US $2,500 for purchases in which a purchase order is required for any purchase at or above this price point. Thus, a Benford's Law test of the two leading digits (specifically, 24) could reveal any anomalies, manipulation or fraud involving this cutoff. It is also useful as a test of controls to see if existing controls for purchase orders are working effectively. It is important to note that since the cutoff amount has two key digits, a two-digit test is needed rather than a single leading digit.

Other objectives are equally applicable, including analysis of:

- Credit card transactions

- Purchase orders
- Loan data
- Customer balances
- Journal entries
- Stock prices
- Accounts payable transactions
- Inventory prices
- Customer refunds
-

Examples of data sets that are not likely to be suitable for Benford's Law include:

- Airline passenger counts per plane
- Telephone numbers
- Data sets with 500 or fewer transactions.
- Data generated by formulas (e.g., YYMM#### as an insurance policy number)
- Data restricted by a maximum or minimum number (e.g., hourly wage rate)

As stated previously, the IT auditor will need to determine whether to run a one-digit test or two-digit test. The two-digit test will usually give more granular results, but is also likely to reveal more spikes than a one-digit test. For certain tests, two digits are critical (see the previous example on purchase order cutoff).

Once the test has been run, the IT auditor will need to determine what results deserve more attention or whether the results provide evidence or information related to the audit objective. Generally speaking, the spikes above the Benford's Law line are the numbers of interest (see 4, not 5, in **figure 2**). The IT auditor will want to obtain independent information on why the digit(s) spike(s). The results that show a digit that is lower than probable occurrence are generally ignored, unless the audit objective is in that direction.

Constraints in Using Benford's Law

The assumptions regarding the data to be examined by Benford's Law are

- Numeric data

- Randomly generated numbers:

  – Not restricted by maximums or minimums

  – Not assigned numbers

- Large sets of data
- Magnitude of orders (e.g., numbers migrate up through 10, 100, 1,000, 10,000, etc.) (Other assumptions exist that are unimportant in applying Benford's Law in IT audits.)

The mathematical theory has always been applied to digital analysis, i.e., a logarithmic study of the occurrence of digits by position in a number.

It is important to note that one assumption of Benford's Law is that the numbers in the large data set are randomly generated. For example, hourly wages will have a minimum and possibly some maximum (even if a realistic maximum) that means that the data set is not generated in a completely random fashion, but rather uses a restricted or manipulated set of digits as the potential leading digit. The same is true if there is a formula or structure to the manner in which the number is generated. For example, US telephone numbers are assigned with a specific area code and a limited number of 3-digit prefaces to the last 4 digits (which are the only truly randomly generated numbers in a phone number). Thus, before applying Benford's Law, the IT auditor should ensure that the numbers are randomly generated without any real or artificial restriction of occurrence.

As can be seen, Benford's Law should be applied only to large data sets. For IT auditors, that would be data such as files with hundreds of transactions (e.g., invoices to customers, disbursements, payments received, inventory items). It is inadvisable to use Benford's Law for small-sized data sets, as it would not be reliable in such cases. Thus, some experts recommend data sets of at least 100 records. This author recommends that the data set be 1,000 records or more, or that the IT auditor justify why a lower volume of transactions is suitable to Benford's Law, i.e., show that the smaller size still meets the other constraints and that size will not affect the reliability of results. The orders of magnitude in particular usually take hundreds of transactions. Using fewer than 1,000 can also lead to too many spikes of interest, too many false positives.

The IT auditor should be careful in extracting a sample and then using Benford's Law on the sample. That is especially true for directed samples in which the amount is part of the factor allowing a transaction to be chosen. This is because the sample is not truly a random sample. For example, pulling a sample of all invoices over US $5,000 leads to a data set that is not random. For small entities, using a data set for the whole month, or a random day of each month, is a better sample for Benford's Law purposes.

Conclusion

Benford's Law can recognize the probabilities of highly likely or highly unlikely frequencies of numbers in a data set. The probabilities are based on mathematical logarithms of the occurrence of digits in randomly generated numbers in large data sets. Those who are not aware of this theory and intentionally manipulate numbers (e.g., in a fraud) are susceptible to getting caught by the application of Benford's Law. The IT auditor can also apply Benford's Law in tests of controls and other IT-related tests of data sets. However, the IT auditor needs to remember to make sure that the constraints (mathematical assumptions of the theory) are compatible with the data set to be tested.

7. Theory of relative size factor (RSF)

It highlights all unusual fluctuations, which may be routed from fraud or genuine errors. RSF is measured as the ratio of the largest number to the second largest number of the given set. In practice there exist certain limits (e.g. financial) for each entity such as vendor, customer, employee, etc. These limits may be defined or analyzed from the available data-if not defined. If there is any stray instance of that is way beyond the normal range, then there is a need to investigate further into it. It helps in better detection of anomalies or outliners. In records that fall outside the prescribed range are suspected of errors or fraud. These records or fields need to relate to other variables or factors in order to find the relationship, thus establishing the truth.

8. Computer Assisted Auditing Tools (CAATs)

CAATs are computer programs that the auditor use as part of the audit procedures to process data of audit significance contained in a client's information systems, without depending on him. CAAT

helps auditors to perform various auditing procedures such as: (a) Testing details of transactions and balances, (b) identifying inconsistencies or significant fluctuations, (c) Testing general as well as application control of computer systems. (d) Sampling programs to extract data for audit testing, and (e) Redoing calculations performed by accounting systems.

9. Data mining techniques

It is a set of assisted techniques designed to automatically mine large volumes of data for new, hidden or unexpected information or patterns. Data mining techniques are categorized in three ways: Discovery, Predictive modeling and Deviation and Link analysis. It discovers the usual knowledge or patterns in data, without a predefined idea or hypothesis about what the pattern may be, i.e. without any prior knowledge of fraud. It explains various affinities, association, trends and variations in the form of conditional logic. In predictive modeling, patterns discovered from the database are used to predict the outcome and to guess data for new value items. In Deviation analysis the norm is found first, and then those items are detected that deviate from the usual within a given threshold (to find anomalies by extracted patterns). Link discovery has emerged recently for detecting a suspicious pattern. It mostly uses deterministic graphical techniques, Bayesian probabilistic casual networks. This method involves "pattern matching" algorithm to 'extract' any rare or suspicious cases.

10. Ratio Analysis

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

Three commonly employed ratios are: -

1. The ratio of the highest value to the lowest value (max/min);
2. The ratio of the highest value to the second highest value (max/max2); and

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

The following strategic fraud detection approach shows how the use of information systems and technology provide effective ways to detect fraud –

(1) understanding the business,

(2) identifying all possible frauds that could occur,

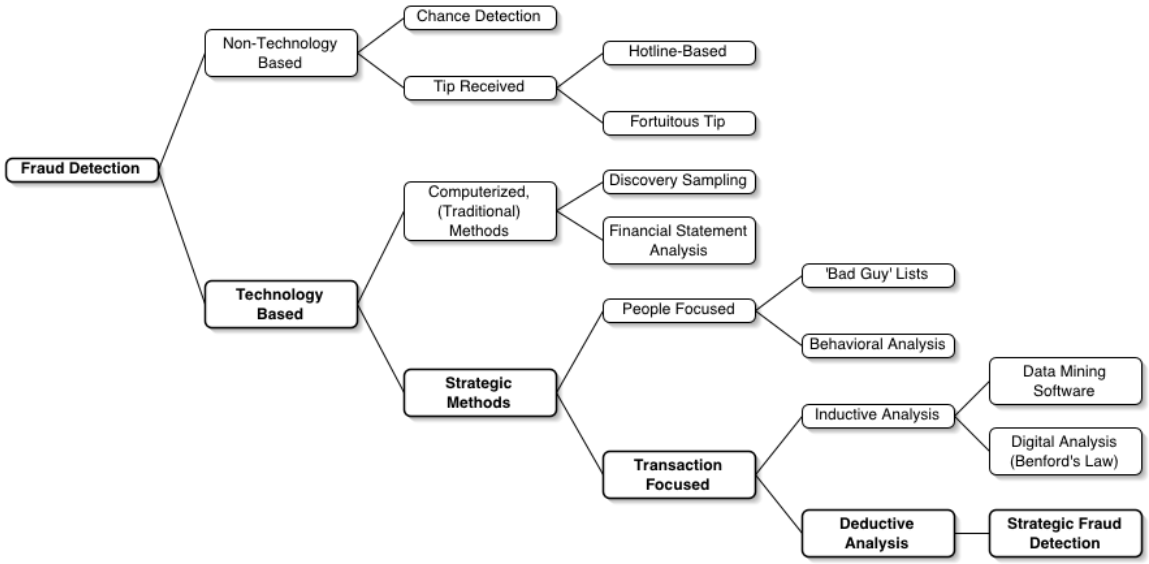
(3) cataloging possible symptoms for each type of fraud,

(4) using technology to gather data about symptoms,

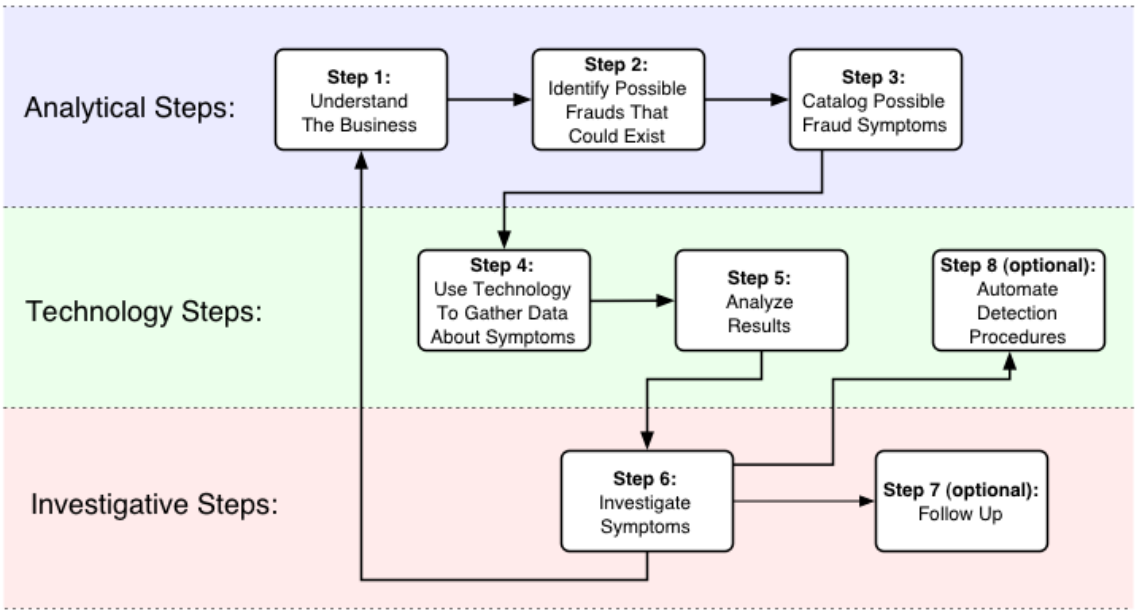
(5) analyzing and refining results, and

(6) investigating identified symptoms

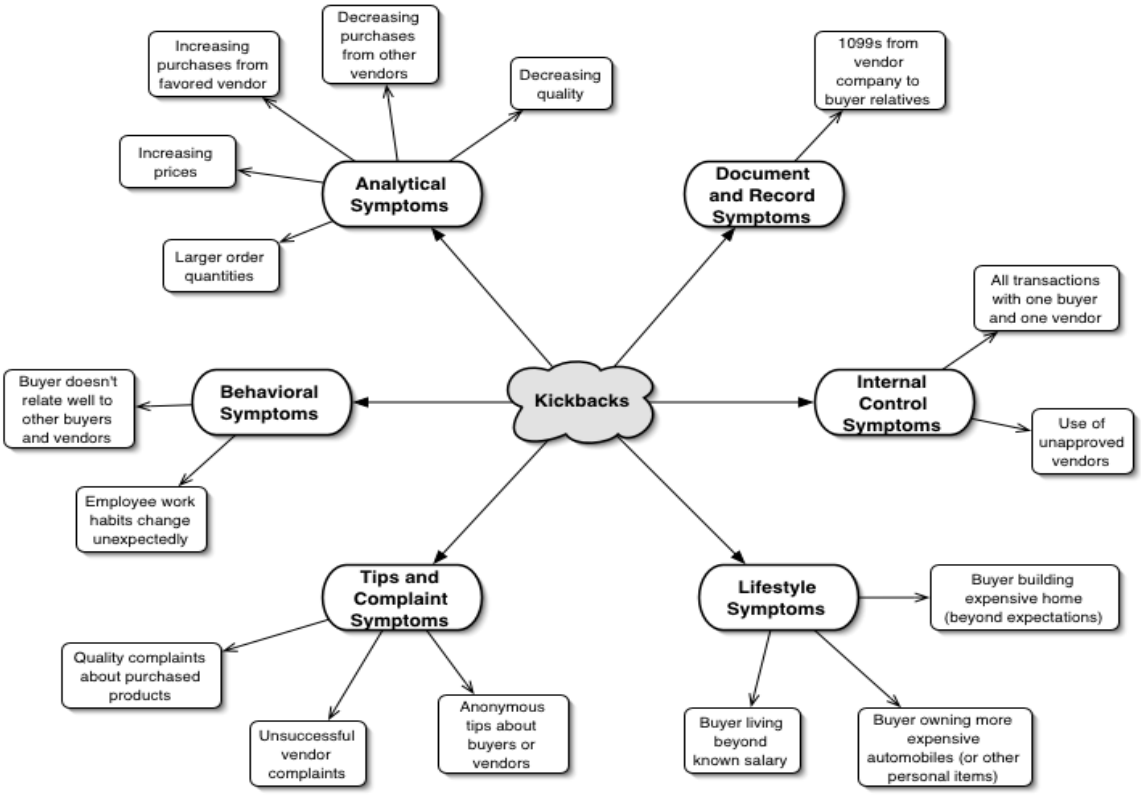
Categorization of Fraud Detection Methods -



Strategic Fraud Detection Approach -



Fraud Symptoms for Kickbacks -



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 is 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 part of the auditor's goal in evaluating the risk that misstatements due to fraud may have occurred.

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

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. 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 Governal-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 fulfill the requirements of time and large amendments were introduced. In 1882, it ware 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 breath 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. 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. 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.[1]

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.

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

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
    - any process, or
    - activity connected,

- with the **Proceeds of Crime,** including its
    - Concealment,
    - Possession,
    - 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
    - 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 being available for creditors, Dishonest or Fraudulent execution of deed of transfer containing false statement of consideration.

- Offences under the Narcotic Drugs and Psychotropic Substances Act, 1985
- Offences under the Prevention of Corruption Act, 1988;
- 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.
- Offences under the Customs Act, 1962 relating to evasion of duty or prohibitions;
- Offences under the Emigration act, 1983
- Offences under the Foreigners act, 1946
- Offences under the Antiquities and Arts Treasures Act, 1972
- 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;
- 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.
- Offences under The Information Technology Act, 2000, including
    - Breach of confidentiality and privacy,
    - Offence or contravention committed outside India.
- 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
    - in charge of, and
    - 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
    - which shall not be less than Three years, but
    - which may extend to 7 years/10 years, and
    - shall also be liable to fine.

In certain cases, the offences under Narcotic Drugs and Psychotropic Substances Act, 1985 are punishable with rigorous imprisonment upto 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
    - Concealed,
    - Transferred, or
    - 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 Organisation (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 authorised dealer,money changer, off-shore banking unit or any other person for the time being authorised 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 to its necessary requirements.

7. The Information Technology Act, 2000

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.

Information technology Act 2000 consisted of 94 sections segregated into 13 chapters. Four schedules form part of the Act. In the 2008 version of the Act, there are 124 sections (excluding 5 sections that have been omitted from the earlier version) and 14 chapters. Schedule I and II have been replaced. Schedules III and IV are deleted.

Information Technology Act 2000 addressed the following issues:

- Legal recognition of electronic documents
- Legal Recognition of digital signatures
- Offenses and contraventions
- Justice dispensation systems for cybercrimes

According to Section 10A of information technology Act,2000(amended in 2008)it also validates E-contracts.

8. The Companies Act, 2013

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

"fraud" in relation to affairs of a company or any body corporate, includes
(a) any act,
(b) omission,
(c) concealment of any fact or
(d) abuse of position committed by any person or any other person with the connivance in any manner, -

- with intent to deceive,
- to gain undue advantage from, or
- to injure the interests of,

- the company or
- its shareholders or
- its creditors or
- any other person,

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

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

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.

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, cyber crimes and major frauds, scams and other white collar offences.

vii. State vigilance Commission

viii. Lokayuktha & Upa Lokayuktha

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 organisation with experts on finance, capital market, accountancy, forensic audit, 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 organisations 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 orderd 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.

Fraud law covers a broad range of crimes and civil tort actions that address situations in which a person wrongfully obtains money, property, or other benefits by deceit. In the criminal context, fraud is typically charged as a felony, meaning that a conviction can result in a year or more of incarceration. Criminal penalties can also include statutory fines, restitution (victim reimbursement), community service, as well as the loss of civil rights associated with a felony conviction. In civil court, financial compensation is generally the plaintiff's sole remedy. Fraud cases can be brought in either state or federal court.

UNITED KINGDOM

Fraud Act, 2006 – United Kingdom

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

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

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

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

- "**Fraud by false representation**" is defined by Section 2 of the Act as a case where a person makes "any representation as to fact or law ... express or implied" which they know to be untrue or misleading.

- "**Fraud by failing to disclose information**" is defined by Section 3 of the Act as a case where a person fails to disclose any information to a third party when they are under a legal duty to disclose such information.

- "**Fraud by abuse of position**" is defined by Section 4 of the Act as a case where a person occupies a position where they are expected to safeguard the financial interests of another person, and abuses that position; this includes cases where the abuse consisted of an omission rather than an overt act.

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

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

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

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

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

Section 12 of the Act provides that where an offence against the Act was committed by a body corporate, but was carried out with the "consent or connivance" of any director, manager,

secretary or officer of the body - or any person purporting to be such - then that person, as well as the body itself, is liable.

Bribery Act, 2010

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

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

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

The Bribery Act creates four prime offences:

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

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

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

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

UK companies doing business overseas -

Companies registered in the UK must take note of the extra-territorial reach of the Bribery Act. A company can commit an offence under section 7 of failure to prevent bribery if an employee, subsidiary, agent or service provider ('associated persons') bribes another person anywhere in the world to obtain or retain business or a business advantage.

A foreign subsidiary of a UK company can cause the parent company to become liable under section 7 when the subsidiary commits an act of bribery in the context of performing services for the UK parent. If the foreign subsidiary were acting entirely on its own account it would not cause the UK parent to be liable for failure to prevent bribery under section 7 as it would not then be performing services for the UK parent.

However, the UK parent might still be liable for the actions of its subsidiary in other ways such as false accounting offences or under the Proceeds of Crime Act 2002.

Foreign companies with operations in the UK -

The Bribery Act has important implications for foreign companies which do business in the UK as its territorial scope is extensive. The corporate offence set out in Section 7 of failure to prevent bribery in the course of business applies to any relevant commercial organisation defined as a body incorporated under the law of the United Kingdom (or United Kingdom registered partnership) and any overseas entity that carries on a business or part of a business in the United Kingdom.

A foreign company which carries on any part of its business in the UK could be prosecuted for failure to prevent bribery even where the bribery takes place wholly outside the UK and the benefit or advantage to the company is intended to accrue outside the UK.

Section 11 explains the penalties for individuals and companies found guilty of committing a crime. If an individual is found guilty of a bribery offence, tried as a summary offence, they may be imprisoned for up to 12 months and fined up to £5,000. Someone found guilty on indictment, however, faces up to 10 years' imprisonment and an unlimited fine. The crime of a commercial organisation failing to prevent bribery is punishable by an unlimited fine. In addition, a convicted individual or organisation may be subject to a confiscation order under the Proceeds of Crime Act 2002, while a company director who is convicted may be disqualified under the Company Directors Disqualification Act 1986.

(The Proceeds of Crime Act 2002 (c.29) (POCA) is an Act of the Parliament of the United Kingdom which provides for the confiscation or civil recovery of the proceeds from crime and contains the principal money laundering legislation in the UK.)

Serious Fraud Office (United Kingdom)

http://www.sfo.gov.uk/

The Serious Fraud Office (SFO) is an independent UK Government department that investigates and prosecutes serious or complex fraud and corruption. Accountable to the Attorney General, it has jurisdiction over England, Wales and Northern Ireland and assists a number of overseas investigations by obtaining information from UK sources. Section 2 of the Criminal Justice Act, 1987 grants the SFO special compulsory powers to require any person (or business/bank) to provide any relevant documents (including confidential ones) and answer any relevant questions including ones about confidential matters.

The SFO is also the principal enforcer of the Bribery Act 2010, which has been designed to encourage good corporate governance and enhance the reputation of the City of London and the UK as a safe place to do business.

The SFO is a specialist organisation that investigates only the most serious types of economic crime. As a result a potential case must meet certain criteria before it is taken on. These criteria include whether -

- the value of the alleged fraud is more than £1 million

- there is a significant international dimension
- the case is likely to be of widespread public concern
- the requires highly specialised knowledge, for example, of financial markets
- the SFO's special powers need to be used

The SFO is unique in that its role is to both investigate and prosecute. Its case teams are therefore made up of investigators, lawyers, law clerks and forensic accountants.

National Fraud Authority (NFA)

https://www.gov.uk/government/organisations/national-fraud-authority

The National Fraud Authority is an executive agency of the United Kingdom Home Office responsible for increasing protection for the UK economy from the harm caused by fraud. The NFA works with a wide range of partners with the aim of making fraud more difficult to commit in the UK. Formerly the National Strategic Fraud Authority, it was set up in October 2008 in response to the government's Fraud Review in 2006. It concluded that fraud is a significantly under-reported crime, and while various agencies and organisations were attempting to tackle the issue, greater co-operation was needed to achieve a real impact within the public sector. The scale of the problem pointed to the need to bring together the numerous counter-fraud initiatives that existed, which is when the NFA was formed.

The NFA works to tackle frauds across the spectrum, but also works on fraud types and fraud issues that are a notable problem. These include identity fraud, mortgage fraud, accommodation addresses, mass marketing fraud and fraud affecting small and medium sized businesses. The NFA also produces the Annual Fraud Indicator, which estimates the cost of fraud. Working with the charity, Victim Support, the NFA has also done some significant work with victims, to ensure they receive the support they deserve if they have been a victim of the crime.

Action Fraud is the UK's national fraud reporting service, run by a private sector company called bss for the National Fraud Authority. Action Fraud is the place to go to get information and advice about fraud, as well as to report fraud. UK citizens can report fraud online (such as forwarding scam emails for inspection) or by telephone. When a fraud is reported to Action Fraud, victims are given a crime reference number and their case is passed on to the National Fraud Intelligence

Bureau (NFIB), which is run by the City of London's police service. The Action Fraud website also has an A-Z of fraud describing different types of fraud, and offers prevention advice.

The National Fraud Authority publishes the **Annual Fraud Indicator** every year, which is the UK's comprehensive estimate of how much fraud costs the UK. The annual fraud indicator for 2012 was published in March 2012, and estimated that fraud would cost the UK over £73 billion that year. This was up from £38 billion in 2011. When broken down by sector, the indicator revealed that fraud losses to the public sector amounted to £20.3 billion, the private sector lost £45.5 billion, the not-for-profit sector lost £1.1 billion and individuals lost £6.1 billion.

CIFAS - The UK's Fraud Prevention Service

http://www.cifas.org.uk/

CIFAS is a not-for-profit membership association representing the private and public sectors. CIFAS is dedicated to the prevention of fraud, including staff fraud, and the identification of financial and related crime. CIFAS operates two databases:

- National Fraud Database (NFD
- Staff Fraud Database (SFD)

CIFAS has 290 Member organisations spread across various business sectors. These include financial services, retail, telecommunications, customer service centres, call centres and public services. Although at present CIFAS Members are predominantly private sector organisations, public sector bodies may also share fraud data reciprocally through CIFAS to prevent fraud.

Members share information about confirmed frauds in the fight to prevent further fraud. CIFAS is unique and was the world's first not-for-profit fraud prevention data sharing organisation. Since CIFAS was founded, CIFAS Members have prevented fraud losses to their organisations worth over £8 billion by sharing fraud data.

CIFAS AIMS TO:

- Build on crime prevention data sharing to encompass both the private and public sectors in the public interest.

- Protect the interests of CIFAS Members from the actions of criminals by pooling information on fraud and prevented fraud.

- Ensure that innocent members of the public who are the victims of fraud are not prejudiced by the misuse of their identities and documentation.

UNITED STATES OF AMERICA

Foreign Corrupt Practices Act, 1977 – United States of America

The Foreign Corrupt Practices Act of 1977 (FCPA) is a United States federal law known primarily for two of its main provisions, one that addresses accounting transparency requirements under the Securities Exchange Act of 1934 and another concerning bribery of foreign officials.

As a result of U.S. Securities and Exchange Commission investigations in the mid-1970s, over 400 U.S. companies admitted making questionable or illegal payments in excess of $300 million to foreign government officials, politicians, and political parties. The abuses ran the gamut from bribery of high foreign officials to secure some type of favorable action by a foreign government to so-called facilitating payments that were made to ensure that government functionaries discharged certain ministerial or clerical duties. One major example was the Lockheed bribery scandals, in which officials of aerospace company Lockheed paid foreign officials to favor their company's products. Another was the Bananagate scandal in which Chiquita Brands had bribed the President of Honduras to lower taxes. Congress enacted the FCPA to bring a halt to the bribery of foreign officials and to restore public confidence in the integrity of the American business system.

The Act was signed into law by President Jimmy Carter on December 19, 1977, and amended in 1998 by the International Anti-Bribery Act of 1998 which was designed to implement the anti-bribery conventions of the Organization for Economic Co-operation and Development.

The FCPA applies to any person who has a certain degree of connection to the United States and engages in foreign corrupt practices. The Act also applies to any act by U.S. businesses, foreign corporations trading securities in the United States, American nationals, citizens, and residents acting in furtherance of a foreign corrupt practice whether or not they are physically present in the United States. In the case of foreign natural and legal persons, the Act covers their actions if

they are in the United States at the time of the corrupt conduct. Further, the Act governs not only payments to foreign officials, candidates, and parties, but any other recipient if part of the bribe is ultimately attributable to a foreign official, candidate, or party. These payments are not restricted to just monetary forms and may include anything of value.

Persons subject to FCPA –

- **Issuers**

  Includes any U.S. or foreign corporation that has a class of securities registered, or that is required to file reports under the Securities and Exchange Act of 1934
- **Domestic concerns**

  Refers to any individual who is a citizen, national, or resident of the United States and any corporation and other business entity organized under the laws of the United States or of any individual US State, or having its principal place of business in the United States
- **Any person**

  covers both enterprises and individuals

The anti-bribery provisions of the FCPA make it unlawful for a U.S. person, and certain foreign issuers of securities, to make a payment to a foreign official for the purpose of obtaining or retaining business for or with, or directing business to, any person. Since 1998, they also apply to foreign firms and persons who take any act in furtherance of such a corrupt payment while in the United States. The meaning of foreign official is broad. For example, an owner of a bank who is also the minister of finance would count as a foreign official according to the U.S. government. Doctors at government-owned or managed hospitals are also considered to be foreign officials under the FCPA, as is anyone working for a government-owned or managed institution or enterprise. Employees of international organizations such as the United Nations are also considered to be foreign officials under the FCPA. There is no materiality to this act, making it illegal to offer anything of value as a bribe, including cash or non-cash items. The government focuses on the intent of the bribery rather than on the amount.

The FCPA also requires companies whose securities are listed in the United States to meet its accounting provisions. These accounting provisions, which were designed to operate in tandem

with the anti-bribery provisions of the FCPA, require corporations covered by the provisions to make and keep books and records that accurately and fairly reflect the transactions of the corporation and to devise and maintain an adequate system of internal accounting controls. An increasing number of corporations are taking additional steps to protect their reputation and reducing exposure by employing the services of due diligence companies. Identifying government-owned companies in an effort to identify easily overlooked government officials is rapidly becoming a critical component of more advanced anti-corruption programs.

Regarding payments to foreign officials, the act draws a distinction between bribery and facilitation or "grease payments", which may be permissible under the FCPA but may still violate local laws. The primary distinction is that grease payments are made to an official to expedite his performance of the duties he is already bound to perform. Payments to foreign officials may be legal under the FCPA if the payments are permitted under the written laws of the host country. Certain payments or reimbursements relating to product promotion may also be permitted under the FCPA.

OECD ANTI-BRIBERY CONVENTION

http://www.oecd.org/daf/anti-bribery/anti-briberyconvention/

The OECD Anti-Bribery Convention (officially Convention on Combating Bribery of Foreign Public Officials in International Business Transactions) is a convention of the OECD aimed at reducing corruption in developing countries by encouraging sanctions against bribery in international business transactions carried out by companies based in the Convention member countries. Its goal is to create a truly level playing field in today's international business environment.

The OECD was founded in 1961 to stimulate economic progress and world trade.

In 1989, the OECD established *ad hoc* working group for comparative review of national legislations regarding the bribery of foreign public officials. In 1994, the OECD Ministerial Council adopted the Recommendation of the Council on Bribery in International Business Transactions; the revised recommendation was adopted in 2007. The *ad hoc* working group was replaced by the OECD Working Group on Bribery in International Business Transactions. The convention was signed on 17 December 1997 and came into force on 15 February 1999.

Countries that have signed the convention are required to put in place legislation that criminalises the act of bribing a foreign public official. The OECD has no authority to implement the convention, but instead monitors implementation by participating countries. Countries are responsible for implementing laws and regulations that conform to the convention and therefore provide for enforcement. The OECD performs its monitoring function in a two-phased examination process. Phase I consists of a review of legislation implementing the conventions in the member country with the goal of evaluating the adequacy of the laws. Phase 2 assesses the effectiveness with which the legislation is applied.

The Convention is open to accession by any country which is a member of the OECD or has become a full participant in the OECD Working Group on Bribery in International Business Transactions. As of May 2013, 40 countries have ratified or acceded to the convention:

Presently India is not a member of the OECD Anti-Bribery Convention.

U.N. CONVENTION AGAINST CORRUPTION

The **United Nations Convention against Corruption** (UNCAC) is a multilateral convention negotiated by members of the United Nations. It is the first global legally binding international anti-corruption instrument. In its 71 Articles divided into 8 Chapters, UNCAC requires that States Parties implement several anti-corruption measures which may affect their laws, institutions and practices. These measures aim at preventing corruption, criminalizing certain conducts, strengthening international law enforcement and judicial cooperation, providing effective legal mechanisms for asset recovery, technical assistance and information exchange, and mechanisms for implementation of the Convention, including the Conference of the States Parties to the United Nations Convention against Corruption (CoSP).

The United Nations Office on Drugs and Crime (UNODC) promotes the convention and its implementation.

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 cyber crime "as arguably the top systemic threat facing global financial markets and associated infrastructure."

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

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

In India, Japan and China, the era of modern computer, however, began with the analytical engine of Charles Babbage. The first spam email took place in 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 Skrenta, developed the EIK Cloner.

CATEGORIES OF CYBER CRIME

We can categorize cyber crime in two ways

- The computer as a target:- using a computer to attacks other computer, e.g. Hacking, virus/worms attacks, Dos attack etc.
- The computer as a weapon:- using a computer to commit real world crime e.g. cyber terrorism, credit card fraud and pornography etc.

TYPES OF CYBER CRIME

Hacking

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

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

court before which the prosecution of such offence is pending and triable by any magistrate.

E-Mail Spoofing

E-mail spoofing is e-mail activity in which the sender addresses and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is sending an e-mail to another person in such a way that it appears that the e-mail was sent by someone else. A spoof email is one that appears to originate from one source but actually has been sent from another source. Spoofing is the act of electronically disguising one computer as another for gaining as the password system. It is becoming so common that you can no longer take for granted that the e-mail you are receiving is truly from the person identified as the sender.
Email spoofing is a technique used by hackers to fraudulently send email messages in which the sender address and other parts of the email header are altered to appear as though the email originated from a source other than its actual source. Hackers use this method to disguise the actual email address from which phishing and spam messages are sent and often use email spoofing in conjunction with Web page spoofing to trick users into providing personal and confidential information.
Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 66-D and Section417, 419 & 465of Indian Penal Code, 1860 also applicable. Email spoofing offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

Identity Theft

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

Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can

suffer various consequences when they are held responsible for the perpetrator's actions. At one time the only way for someone to steal somebody else's identity was by killing that person and taking his place. It was typically a violent crime. However, since then, the crime has evolved and today's white collared criminals are a lot less brutal. But the ramifications of an identity theft are still scary.

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

Child Pornography

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

LIST OF TOP 20 COUNTRIES WITH THE HIGHEST RATE OF CYBER CRIME (SOURCE: BUSINESS WEEK / SYMANTEC)

1. United States of America

Share of malicious computer activity: 23%

Malicious code rank: 1

Spam zombies rank: 3

Phishing web site hosts rank: 1

Bot rank: 2

Attack origin rank: 1

2. China

Share of malicious computer activity: 9%

Malicious code rank: 2

Spam zombies rank: 4

Phishing web site hosts rank: 6

Bot rank: 1

Attack origin rank: 2

3. Germany

Share of malicious computer activity: 6%

Malicious code rank: 12

Spam zombies rank: 2

Phishing web site hosts rank: 2

Bot rank: 4

Attack origin rank: 4

4. Britain

Share of malicious computer activity: 5%

Malicious code rank: 4

Spam zombies rank: 10

Phishing web site hosts rank: 5

Bot rank: 9

Attack origin rank: 3

5. Brazil

Share of malicious computer activity: 4%

Malicious code rank: 16

Spam zombies rank: 1

Phishing web site hosts rank: 16

Bot rank: 5

Attack origin rank: 9

6. Spain

Share of malicious computer activity: 4%

Malicious code rank: 10

Spam zombies rank: 8

Phishing web site hosts rank: 13

Bot rank: 3

Attack origin rank: 6

7. Italy

Share of malicious computer activity: 3%

Malicious code rank: 11

Spam zombies rank: 6

Phishing web site hosts rank: 14

Bot rank: 6

Attack origin rank: 8

8. France

Share of malicious computer activity: 3%

Malicious code rank: 8

Spam zombies rank: 14

Phishing web site hosts rank: 9

Bot rank: 10

Attack origin rank: 5

9. Turkey

Share of malicious computer activity: 3%

Malicious code rank: 15

Spam zombies rank: 5

Phishing web site hosts rank: 24

Bot rank: 8

Attack origin rank: 12

10. Poland

Share of malicious computer activity: 3%

Malicious code rank: 23

Spam zombies rank: 9

Phishing web site hosts rank: 8

Bot rank: 7

Attack origin rank: 17

11. India

Share of malicious computer activity: 3%

Malicious code rank: 3

Spam zombies rank: 11

Phishing web site hosts rank: 22

Bot rank: 20

Attack origin rank: 19

12. Russia

Share of malicious computer activity: 2%

Malicious code rank: 18

Spam zombies rank: 7

Phishing web site hosts rank: 7

Bot rank: 17

Attack origin rank: 14

13. Canada

Share of malicious computer activity: 2%

Malicious code rank: 5

Spam zombies rank: 40

Phishing web site hosts rank: 3

Bot rank: 14

Attack origin rank: 10

14. South Korea

Share of malicious computer activity: 2%

Malicious code rank: 21

Spam zombies rank: 19

Phishing web site hosts rank: 4

Bot rank: 15

Attack origin rank: 7

15. Taiwan

Share of malicious computer activity: 2%

Malicious code rank: 11

Spam zombies rank: 21

Phishing web site hosts rank: 12

Bot rank: 11

Attack origin rank: 15

16. Japan

Share of malicious computer activity: 2%

Malicious code rank: 7

Spam zombies rank: 29

Phishing web site hosts rank: 11

Bot rank: 22

Attack origin rank: 11

17. Mexico

Share of malicious computer activity: 2%

Malicious code rank: 6

Spam zombies rank: 18

Phishing web site hosts rank: 31

Bot rank: 21

Attack origin rank: 16

18. Argentina

Share of malicious computer activity: 1%

Malicious code rank: 44

Spam zombies rank: 12

Phishing web site hosts rank: 20

Bot rank: 12

Attack origin rank: 18

19. Australia

Share of malicious computer activity: 1%

Malicious code rank: 14

Spam zombies rank: 37

Phishing web site hosts rank: 17

Bot rank: 27

Attack origin rank: 13

20. Israel

Share of malicious computer activity: 1%

Malicious code rank: 40

Spam zombies rank: 16

Phishing web site hosts rank: 15

Bot rank: 16

Attack origin rank: 22

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

Cyber Law of India

Cyber crime can involve criminal activities that are traditional in nature, such as theft, fraud, deformation and mischief, all of which are subjected to the India Penal code. In simple way we can say that cyber crime is unlawful acts where in the computer is either a tool or both. The abuse of computer has also given birth of new age crimes that are addressed by the Information Technology Act, 2000.

The offences included in the IT Act 2000 are as follows:

1. Tampering with the computer source documents.

2. Hacking with computer system.

3. Publishing of information which is obscene in electronic form.

4. Power of Controller to give directions

5. Directions of Controller to a subscriber to extend facilities to decrypt information

6. Protected system

7. Penalty for misrepresentation

8. Penalty for breach of confidentiality and privacy

9. Penalty for publishing Digital Signature Certificate false in certain particulars

10. Publication for fraudulent purpose

11. Act to apply for offence or contravention committed outside India

12. Confiscation

13. Penalties or confiscation not to interfere with other punishments.

14. Power to investigate offences.

Major Offences under the It Act 2000

Section 65: Tampering with computer source documents:

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer Programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation: For the purpose of this section "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Section66: Hacking with the computer system

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Section 67: Publishing of obscene information in electronic form

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstance, to read see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

Section 68: Power of controller to give directions

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

Section 69: Directions of Controller to a subscriber to extend facilities to decrypt information:

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence; for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber 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 decrypt the information.

The subscriber or any person who fails to assist the agency referred to in subsection shall be punished with an imprisonment for a term which may extend to seven years.

Section 70: Protected System

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provision of this section shall be punished with imprisonment of either description for a term which may extend to ten 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 Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or which fine which may extend to one lakh rupees, or with both.

Section 72: Penalty for breach of confidentiality and privacy

Save as otherwise provide in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulation made there under, has secured assess to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such 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 73: Penalty for publishing Digital Signature Certificate false in certain particulars

(1) No person shall publish a Digital 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.

(2) 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 75: Act to apply for offence or contravention committed outside India

(1) 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.

(2) 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.

FORENSIC AUDIT IN DIGITAL ENVIORNMENT

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.

Techniques used for detection of fraud

Data Mining

In 2002, Gene Morse found a round $500 million debit to a PP&E account at WorldCom. He discovered the anomaly through searches in a custom data warehouse he had developed in the Essbase multidimensional database. WorldCom would not give Morse access to full financial systems, so he created his own warehouse and used basic data mining techniques to search it. Using a small script and Microsoft Access, Morse followed the account through the financial reporting system and ultimately discovered a $1.7 billion entry of capitalized line costs in 2001.

The WorldCom fraud discovery is one example of using computer technology to search full populations of data for anomalies, trends, and fraud. Traditional auditing uses techniques like discovery, stratified, or random sampling to determine whether a population contains errors (Albrecht and Albrecht, 2002). This approach works well when auditors are searching for anomalies—unintentional errors usually caused by weaknesses in controls because anomalies occur at regular intervals throughout the data set. In contrast, fraud intentional errors caused by intelligent human being can occur in only a few transactions. While a sample of a population containing anomalies should be representative, a sample of a population containing fraud may not be representative.

Assuming a fraud is recorded in only a few transactions, a sampling rate of 5 percent results in a 95 percent risk the fraud will not be sampled and will be missed. Fraud detection methods should

use full populations whenever possible, and since full populations can be voluminous, they almost always require computers and data mining techniques.

Methodology

One of the assumptions that underlie traditional auditing methods is the presence of an intelligent human being. When an auditor checks items in a sample, he or she is able to apply human reason and common sense to transactions. Fraud investigations often start with the auditor conducting a routine audit task, looking at a transaction, and saying, "that doesn't make sense." This approach can be seen as an inductive approach; the auditor investigates further when anomalies are found.

Data mining routines—run by computer—do not have this innate sense of normality. Queries and scripts do exactly what they are programmed to do. They do not "dig deeper" unless the user specifically programs them to do so. To accommodate this limitation, the fraud hypothesis testing approach has been proposed (Albrecht, et. al., 2000). This approach has also been labeled the deductive or proactive approach to fraud detection; it involves the following six step approach.

Auditors gain a solid understanding of the business processes, controls, and environment. This understanding allows them to proactively predict the frauds that might be occurring.

The team brainstorms the possible frauds that could exist in the environment they are auditing. This might result in 50 potential schemes.

Once potential schemes are identified, the team outlines the ways these schemes would show up in data. These indicators, or red flags, are the primary indicators that the fraud may be occurring.

For each indicator, the team searches corporate databases using queries, scripts, and data mining techniques. Any anomalous transactions are pulled for further investigation. This could be seen as a "sample" (albeit not in the traditional sense) that should be looked at more closely.

Auditors analyze the query results to determine possible explanations for the anomalies, which could be fraud, weak controls, or other reasons.

The team follows up on those indicators that may be caused by fraud. These further investigations employ additional queries or traditional means to determine the true cause of the anomalies.

Continuous Auditing

Once computer queries and scripts are written, continuous auditing is possible. Rather than testing on historical data (the normal audit process), tests can be programmed into live corporate systems to provide continuous monitoring of transactions. Continuous monitoring using information technology has been successfully used at a number of companies.

Digital Analysis

Benford's Law works because nature produces more small things than large things. There are more insects than large mammals, more small houses than large ones, and more small lakes than large bodies of water. Similarly, businesses produce more transactions with small amounts than with large amounts. Benford's Law predicts that amounts will start with the digit 1 more often than the digit 9, and it even provides a mathematical formula describing the law and percentages. The digit 1 should show up about 30 percent of the time, while the digit 9 should occur less than 5 percent of the time.

The primary limitation to Benford's Law is business data do not always follow natural patterns; there exist a large number of reasons that transactions may not match Benford's Law. Explanations like recurring fixed expenses, unusual business cycles, and assigned amounts are often found. The author has taught digital analysis to thousands of professional auditors; in ten years of asking participants about their success with digital analysis, only three individuals have reported finding fraud with Benford's Law (others have reported that digital analysis could have been used to find already discovered frauds, but hind sight is not prediction). In some ways, the audit field may have overestimated the usefulness of digital analysis. But despite its limitations, Benford's Law remains one of the most popular data mining techniques for fraud.

Outlier Detection

One of the primary methods of detecting fraud is discovering data values that are outside the normal course of business. For example, a kickback scheme might be the reason purchases from one vendor are twice as high as similar purchases from another vendor.

The simplest method of outlier detection is the statistical z-score calculation. This formula, given as (value mean)/ standard deviation, provides a simple and compact method of measuring

outliers. The numerator shifts each point to a zero based scale, and the denominator adjusts the distribution to a standard deviation of one. Once the data are transformed into this standardized scale, generalized statements can be made. In the author's experience, outlier scores of 5, 8, or even 12 are often found in real world data.

At times these may be the result of non-normal distributions, but even in those cases, the score provides an indicator to potential problems.

More advanced techniques have been used in specialized areas. For example, credit card fraud can be discovered by identifying transactions through both unsupervised and supervised learning. Bolton and Hand (2001) used behavioral outlier detection with unsupervised learning to detect abnormal spending behavior as well as increased frequency of use. Others have used regression models, Discrete Gaussian Exponential, depth based techniques, distance based techniques, and a number of other techniques to identify outliers.

Trending

In addition to comparing same period numbers from different vendors, employees, or customers, fraud can be discovered by comparing numbers over time. Because almost all perpetrators are greedy (Albrecht, 2008), fraud increases exponentially over time. Auditors can easily spot an increasing trend on a line chart computers are not needed if only one item is being audited (one employee, one vendor, etc.). The need for automation is during the initial phase of a fraud investigation. If auditors do not know which item is increasing, they must look through thousands of graphs to determine which item requires additional investigation. Trending methods allow the computer to determine which trends are increasing so the auditor can focus on those items.

One of the most basic methods of determining an increasing trend is linear regression. Once the computer fits a line to the data, the slope and goodness of fit provide a simple measure of trend.

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 auditor 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 accounting 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 recommend 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

SAMPLE TABLE OF CONTENTS (FORENSIC AUDIT REPORT)

EXECUTIVE SUMMARY

1.0 BACKGROUND

1.1 Origin of the Audit

1.2 Audit Objective

1.3 Proposed Audit Outputs

1.4 Audit Implementation Approach

2.0 RISK ANALYSIS

2.1 Internal Environment Risk

2.1.1 Financial Management

2.1.2 Customers, Products and Competitors

2.1.3 Information technology

2.1.4 Business Process

2.1.5 Human Resource Management

2.2 External Environment Forces

2.2.1 Influence of Economics and Loans Market

2.2.2 Political and Legal Scenario

2.2.3 Technology in Banking

3.0 EVIDENCE OF RISK EVENTS

3.1 Conflicts of interest

3.2 Bribery

3.3 Extortion

3.4 Cash theft

3.5 Fraudulent disbursements

3.6 Inventory frauds

3.7 Misuse of assets

3.8 Financial Statement fraud

4.0 AUDIT RECOMMENDATIONS

4.1 Logical Framework Approach

4.2 Preconditions and Risks

5.0 GOVERNANCE ON RECOMMENDATION IMPLEMENTATION

5.1 Stakeholders

5.2 Budget Considerations

List of Annexes

Annex 1: Members of the Interviews

Annex 2: Organization Chart of Bank

Annex 3: Financial Performance (YYYY to YYYY)

Annex 4: Audit Recommendation Logical Framework

Annex 5: Analysis of Key Risk Events

Many Others:

WORKING PAPERS

A forensic accounting 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 accounting 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 accounting 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 auditing 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 auditors 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.

1) Indian Coal Allocation Scam – 2012 – Size 1.86 L Crore

While many think that 2G scam remains the biggest one in size in India. But this coal allocation scam dwarfs it by the amount involved. This scam is in regards to Indian Government's allocation of nation's coal deposit to PSU's and private companies. The scam happened under Manmohan Singh government and came out in 2012.

The basic premise of this scam was the wrongful allocation of Coal deposits by Government without resorting to competitive bidding, which would have made huge amounts to the Government (to the tune of 1.86 Lakh crore). However, the coal deposits were allocated arbitrarily.

2) 2G Spectrum Scam – 2008 – 1.76 L Crore

We have had a number of scams in India; but none bigger than the scam involving the process of allocating unified access service licenses. At the heart of this Rs.1.76-lakh crore worth of scam is the former Telecom minister A Raja – who according to the CAG, has evaded norms at every level as he carried out the dubious 2G license awards in 2008 at a throw-away price which were pegged at 2001 prices.

In some respects, this remains the biggest scam in India if you consider the inflation. The 2G spectrum allocation happened 5 years earlier than Coal Scam which came out in 2012.

The cases are still going on against many people including A. Raja, M. K. Kanimozhi and many telecommunication companies as well.

3) Wakf Board Land Scam – 2012 – 1.5-2L Crore

In March of 2012, Anwar Maniapddy, the chairman of Karnataka State Minorities Commission submitted a sensational report which alleged 27,000 acres of land, which was controlled by Karnataka Wakf Board had been allocated illegally or misappropriated. The value of land which was misappropriated was in tune of 1.5 to 2 lakh crore rupees.

The land managed by Wakf board, a Muslim charitable trust, is typically donated to under-privileged and poor people of Muslim community. However, the report alleged that nearly 50 percent of the land owned by Wakf board was misappropriated by Politicians and Board members in conjunction with real estate mafia at fraction of actual land cost.

The investigations for this are currently ongoing.

4) Commonwealth Games Scam – 2010 – 70,000 Crore

Another feather in the cap of Indian scandal list is Commonwealth Games loot. Yes, literally a loot! Even before the long awaited sporting bonanza could see the day of light, the grand event was soaked in the allegations of corruption.

It is estimated that out of Rs. 70000 crore spent on the Games, only half the said amount was spent on Indian sportspersons. The Central Vigilance Commission, involved in probing the alleged corruption in various Commonwealth Games-related projects, has found discrepancies in tenders – like payment to non-existent parties, willful delays in execution of contracts, over-inflated price and bungling in purchase of equipment through tendering and misappropriation of funds.

5) Telgi Scam – 2002 - 20,000 Crore

As they say, every scam must have something unique in it to make money out of it in an unscrupulous manner- and Telgi scam had all the suspense and drama that the scandal needed to thrive and be busted. Abdul Karim Telgi had mastered the art of forgery in printing duplicate stamp papers and sold them to banks and other institutions. The tentacles of the fake stamp and stamp paper case had penetrated 12 states and was estimated at a whooping Rs. 20000 crore plus. The Telgi clearly had a lot of support from government departments that were responsible for the production and sale of high security stamps.

6) Satyam Scam – 2009 – 14,000 Crore

The scam at Satyam Computer Services is something that will shatter the peace and tranquility of Indian investors and shareholder community beyond repair. Satyam is the biggest fraud in the corporate history to the tune of Rs. 14000 crore.

The company's disgraced former chairman Ramalinga Raju kept everyone in the dark for a decade by fudging the books of accounts for several years and inflating revenues and profit figures of Satyam. Finally, the company was taken over by Tech Mahindra which has done wonderfully well to revive the brand Satyam.

7) The Fodder Scam – 1990s - 1,000 Crore

you haven't heard of Bihar's fodder scam of 1996, you might still be able to recognize it by the name of "Chara Ghotala," as it is popularly known in the vernacular language. In this corruption scandal worth Rs.900 crore, an unholy nexus was traced involved in fabrication of "vast herds of fictitious livestock" for which fodder, medicine and animal husbandry equipment was supposedly procured.

8) Bofors Scam – 1980s & 90s – 100 to 200 Crore

The Bofors scandal is known as the hallmark of Indian corruption. The Bofors scam was a major corruption scandal in India in the 1980s; when the then PM Rajiv Gandhi and several others including a powerful NRI family named the Hindujas, were accused of receiving kickbacks from Bofors AB for winning a bid to supply India's 155 mm field howitzer.

The Swedish State Radio had broadcast a startling report about an undercover operation carried out by Bofors, Sweden's biggest arms manufacturer, whereby $16 million were allegedly paid to members of PM Rajiv Gandhi's Congress.

Most of all, the Bofors scam had a strong emotional appeal because it was a scam related to the defense services and India's security interests.

9) The Hawala Scandal – 1990-91 – 100 Crore

The Hawala case to the tune of $18 million bribery scandal, which came in the open in 1996, involved payments allegedly received by country's leading politicians through hawala brokers. From the list of those accused also included Lal Krishna Advani who was then the Leader of Opposition.

Thus, for the first time in Indian politics, it gave a feeling of open loot all around the public, involving all the major political players being accused of having accepted bribes and also alleged connections about payments being channeled to Hizbul Mujahedeen militants in Kashmir.

10) Harshad Mehta & Ketan Parekh Stock Market Scam–1992–5000 Crore combined

Although not corruption scams, these have affected many people. There is no way that the investor community could forget the unfortunate Rs. 4000 crore Harshad Mehta scam and over Rs. 1000 crore Ketan Parekh scam which eroded the shareholders wealth in form of big market jolt.

FORENSIC AUDIT 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.

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)

BAILEY BOOKS INCORPORATED

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 colu 2.	(2) Reasons	(3) File case No.	Entered		Departed	
			Time	Date	Time	Date

APPENDIX A

FRAUD EXAMINATION CHECKLIST

Case Name: _____ Case No.: _____

S.No.	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 canceled cheques? - Identified all bank accounts - Identified number of exemptions - Identified who might be endorsing cheques		
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? - Drivers 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 • 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		
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? - 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 EXAMINAATION CHECKLIST

Case Name: _____ Case No.: _____

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 • 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 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		

	• <u>Boats Owned:</u> Lien holder • <u>Aircraft Owned:</u> Lien holder		
5.	**PUBLIC RECORDS – BUSINESS** - Utility records - UCC Filings - 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.: _____

Neutral Witnesses:

Name	Phone	Date Contacted	Interview Completed	Report Date

APPENDIX A

FRAUD EXAMINATION CHECKLIST

Case Name: _____ Case No.: _____

Adverse Witnesses:

Name	Phone	Date Contacted	Interview Completed	Report Date

APPENDIX A

FRAUD EXAMINATION CHECKLIST

Case Name: _____ Case No.: _____

Co-Conspirators:

Name	Phone	Date Contacted	Interview Completed	Report Date

APPENDIX A

FRAUD EXAMINATION CHECKLIST

Case Name: _____ Case No.: _____

Suspects:

Name	Phone	Date Contacted	Interview Completed	Report Date

SAMPLE DOCUMENT RETENTION POLICY

This is only a SAMPLE DOCUMENT RETENTION POLICY ("DRP"), and is NOT LEGAL ADVICE. It is only an example of a general DRP and should not be used without revision to meet the particular administrative and legal needs of your organisation. There are many federal, state and local laws that require organizations to retain documents for a certain period of time that may not represented in this sample policy. All companies should counsel licensed to practice law in their state before implementing a DRP

1. Purpose:

To ensure the most efficient and effective operation of ORGANIZATION ("organization"), we are implementing this document retention policy ("DRP" or "Policy"). The records of organization and its subsidiaries are important to the proper functioning of organization. Our records include virtually all of the records you produce as an organisation employee. Such records can be in electronic or paper form. Thus, items that you may not consider important such as interoffice emails, desktop calendars and printed memoranda are records that are considered important under this policy (e.g. what records to retain or destroy, when to do so, or how) it is your responsibility to seek answers from organization's DRP manager.

The goals of this DRP are to:

1. Retain important documents for reference and future use;

2. Delete documents that are no longer necessary for the proper functioning of organization;

3. Organize important documents for efficient retrieval; and

4. Ensure that you, as an organisation employee, know what documents should be retained, the length of their retention, means of storage, and when and how they should be destroyed.

Federal and state law requires organization to maintain certain types of records for particular periods. Failure to maintain such records could subject you and organization to penalties and fines, obstruct justice, spoil legal evidence, and / or seriously harm organizations position in litigation. Thus, it is imperative that you fully understand and comply with this, and any future records retention or destruction policies and schedules UNLESS you have been notified by organisation, or if you believe that:

1. Such records are or could be relevant to any future litigation,

2. There is a dispute that could lead to litigation, or

3. Organization is a party to a lawsuit; in which case you MUST PRESERVE such records until organization are legal counsel determines that the records are no longer needed.

"Records" discussed herein refers to all business records of Organization (and is used interchangeably with documents), including written, printed and recorded materials as well as electronic records (i.e. emails, and documents saved electronically). All business records shall be retained for a period no longer that necessary for the purpose conduct and functioning of organization. No business records shall be retained longer than five years, except those that;

1. Have periods provided for herein,

2. are in the document retention schedule, found at Appendix "A" or

3. are specifically exempted by organization's DRP Manager

II. Management

To ensure compliance with this DRP, Organization's DRP manager is responsible for the following oversight functions:

- Implementing the DRP
- Ensuring the employees are properly educated, understand, and follow the DRP's purpose;
- Providing oversight on actual retention and destruction of documents;
- Ensuring the proper storage of documents
- Periodically following up with the counsel to ensure proper retention period are in place;
- Ensuring the proper storage of documents;
- Suspending the destruction of documents upon foreseeable litigation; and
- Keeping corporate officers, directors, and employees apprised of changes in relation to the DRP.

Organization's DRP manager shall annually review the DRP, Modify it accordingly and inform and educate all organization employees on any such changes. All Questions relating to document retention and/or destruction should be directly addressed to organizations DRP manager

III. Types of Records

Appendix "A", Attached at the end of this DRP, Lists several categories of records, as well as specific records that certain specific retention periods. Document retention schedule ("DRS"). All records not provided for in the DRS or described herein, shall be classified into three types,

1. Temporary records

2. Final records

3. Permanent records.

Temporary Records

Temporary records include all business documents that have not been completed. Such include, but are not limited to written memoranda and dictation to be typed in the future, reminders, to do lists, report, case study, and calculation drafts, and interoffice correspondence regarding a client or business transaction and running logs. Temporary records can be destroyed, or permanently deleted if in electronic form (see protocol below for the proper destruction of data in electronic form) when a project/ case/ file, gather and review all such temporary records. Before you destroy or permanently delete these documents, make sure you have duplicates of all the final records pertaining to the project/case/ file. Upon destruction of deletion organize the final records (and duplicates) in a file marked "FINAL" and store them appropriately.

Final Records

Final records include all business documents that are not superseded by modification or addition. Such include, but are not limited to: documents given (or sent via electronic form) to any third party not employed by organisation, or government agency; final memoranda and reports; design/ plan specifications; journal entries; cost estimates; etc. all accounting records shall be deemed final.

Except as provided for in the DRS, all final documents are to be discarded 10 years after the close of a project/ case/ file.

Permanent Records

Permanent records include all business documents that define organization's scope of work,

Expression of professional opinions, research and reference materials. Such include, but are not limited to contracts, proposals, and materials referencing expert opinions annual financial statements, federal tax return, payroll registers, copyright registrations, patents, etc.

Except as provided for in the DRS (Appendix "A") all permanent documents are to be retained indefinitely

Accounting and Corporate Tax Records

Accounting and corporate tax records include, but are not limited to: financial statements; ledgers; audit records; invoices and expense records; federal, state, and property tax returns; payroll; accounting procedures; gross receipts; customer records; purchase; etc.

Unless otherwise specified in the DRS. Such records should be retained for the minimum of 6 years or until the statute of limitations for a particular records expires (please consult organization's counsel for time periods if you manage/ control such records.)

Workplace Records

Workplace records include, but are not limited to article of incorporation, bylaws, meeting minutes, deed and titles, leases, policy statements contracts and agreements, patents and trademark records, etc.

Unless otherwise specified in the DRS, such records should be retained in perpetuity

Employment, Employee, and Payroll Records

Employment records include, but are not limited to job announcements and advertisements; employment applications, background investigations, resumes, and letters of recommendation of persons not hired; etc.

Unless otherwise specified in the DRS. Such records should be retained for the minimum of 1 year

Employee records include, but are not limited to employment applications, background investigations, resumes and letter of recommendation of current and past employees records relating to current and past employee's performance review and complaints, etc.

Unless otherwise specified in the DRS, such records should be retained for the minimum of 3 years following unemployment with organization.

Payroll records include, but are not limited to wage rate tables; salary history; current rate of pay; payroll deductions; time cards; w-2 and w-4 forms; bonuses; etc

Unless otherwise specified in the DRS, such records should be retained for the minimum of 6 (six) years.

Bank Records

Bank records include, but not limited to bank deposits; check copies; stop payment orders; bank statements, cheque signature authorizations, bank reconciliations etc.

Unless otherwise specified in the DRS, such records should be retained for the minimum of 3 years.

Legal Records

Legal records include, but are not limited to all contracts, legal records, statements and correspondence, trademark and copyright registrations patent, personal injury records and statement, press releases, public findings etc.

Unless otherwise specified in the DRS, such records should be retained for the minimum of 10 years.

Historical Records

Historical records are those records that are no longer of use to organization but by virtues of their age or research value may be of historical interest or significance to organization.

Historical records should be retained indefinitely.

IV. Storage

Tangible Records

Tangible records are those in which you must physically move to store, such as paper records (including records printed version of electronically saved documents), photographs, audio

recordings, advertisements and promotional items. Active records and records that need to be easily accessible may be stored in organization's office space or equipment. Inactive records can be sent to organizations offsite storage facility.

Electronic Records

Electronic mail should be either printed and stored as tangible evidence, or downloaded to a computer file and kept electronically or on a disk.

Organization has computer software that duplicate file, which are then backed up on central servers. If you have a notebook computer from organization that you work on out of the office, your computer contains synchronization software that duplicates and back up files when you long into the network. However, it is important that all employees take precautionary measures to save work and records on organization's network drive.

If you save sensitive or important records on computer disks, you should duplicate the information in an alternate format because disks are easily lost or damaged.

V. **Destruction/ Deletion**

Tangible records

Tangible Records should be destroyed by shredding or some other means that will render them unreadable. If you have a record that you do not know how to destroy, such as a photograph, compact disk, or tape recording, ask the advice of organization's DRP manager.

Electronic Records

E-Mails records that you delete remain in organizations system. Thus organization's information technology department will be responsible for permanently removing delete emails from the computer system.

Deleting files and emptying the recycle bin is usually sufficient in most circumstances to get rid of a record. However because electronic records can be stored in many locations, organization's IT department will be responsible for permanently removing deleted files from the computer system.

Keep in mind, where duplicate records are involved, both copies must be destroyed/ deleted where proper.

VI. Cessation of record Destruction/ Deletion

If a lawsuit is filed or imminent, or a legal document request has been made upon organization, *ALL RECORD DESTRUCTION MUST CEASE IMMEDIATELY.* Organization's DRP manager may suspend this DRP to require that documents relating to the lawsuit or potential legal issue(s) be retained and organized. A critical understanding of this section is imperative. Should you fail to follow this protocol, you and/ or organization may be subject to fines and penalties, among other sanctions.

VII. Acknowledgement

I have read and understand the purpose of DRP. I understand that strict adherence to this DRP is a condition of my employment with the organization. If I do not understand something regarding this DRP, I will contact Organization's DRP Manager immediately for clarification. I Agree to Abide by Organization's DRP.

_____ _____

Employee's Signature Date

_____

Employee's Name (Print)

USEFUL WEBSITES

http://www.sfo.gov.uk/ - Serious Fraud Office - UK

https://www.gov.uk/government/organisations/national-fraud-authority - National Fraud Authority – UK

http://www.actionfraud.police.uk/ - Action Fraud - UK

http://www.cifas.org.uk/ - UK's Fraud Prevention Service

http://www.acfe.com/ - Association of Certified Fraud Examiners

http://www.fbi.gov/scams-safety/fraud/fraud - FBI Home page for Fraud

http://www.justice.gov/criminal/fraud/ - The United States department of Justice – Fraud section

http://sfio.nic.in/websitenew/main2.asp - Serious Fraud Investigation Office, India

http://ec.europa.eu/anti_fraud/investigations/report-fraud/ - European Anti-Fraud Office

TEAM MEMBERS

Rajkumar S. Adukia
CFE,(B.Com (Hons), FCA, ACS, Dip in Criminology, LL.B, ACMA, MBA, Dip IFRS (UK), DLL&LP, DIPR)

Ramesh Sambasivan
B.Com, FCA

A.S. Visalakshi
B.Com, FCA,DISA

Pankaj Adukia
B.Com, FCA, LLB, ACS, Dip. IFRS

Shiva Chaudhari
B.Com, FCA, CS, DIBF, FAFE(IFS), MBA

Sini Thomas
B.Com, ACA

Rishabh Adukia
B.Com, ACA, ACS, LLB, Certified Financial PlannerCM

Amit Brahmkhatri
B.Com, ACA

Niraj Mahajan
B.Com, ACA

Samiksha Adukia
B.Com, ACS

Darmesh Kumar
B.Com, ACA

About Global Forensic Audit & Investigation

MBCPL is more than 30 years old company providing consultancy services in field of Business start up, IFRS, IPSAS, Carbon Credit, Real Estate, Auditing and corporate compliance. At MBCPL, we have carved a niche for ourselves in the field of financial and legal expertise be it accounting, auditing or legal compliance. With our ever growing enthusiasm we have developed the field.

Services

Forensic Audit	Business Intelligence	IT Forensic	Advisory
• Financial statement fraud, asset misappropriation, intellectual property theft, white collar crime • Procurement, logistics, outsourcing, vendors/ contractors fraud • Anti-fraud programs	• Due Diligence • Market intelligence • Mystery shopping • Asset tracing • Business partner intelligence	• Digital forensic examination & analysis • Data analytics, solutions • E-Discovery • Cyber-crime prevention, and investigations	• Due diligence and risk assessments • Implementation and monitoring of compliance programs • Business partner risk framework and training • Anti-corruption investigations

Industry Expertise

- Banking
- Insurance
- Chemicals
- Consumer
- Energy
- Healthcare & Hospitality
- Infrastructure
- Logistics
- Oil & Gas
- Real estate
- Retail
- Technology
- Telecom
- Textiles

Our Values & Commitments

Committed to:

- Place the interest of client before ours.
- Service
- Uphold high standards of honesty and integrity
- Endeavour to improve the quality of services
- Excellence in professional services
- Continuous education and staff training

Our Values

- **Teamwork**
- **Learning**
- **Integrity**
- **Accountability**
- **Result oriented**
- **Open to change**
- **Lateral Thinking**

Global Forensic Audit & Investigation
Office- 6, Building No.1, ground Floor, Meridien Apartment,
Veera Desai Road, Andheri (w) Mumbai-400058, India
Ph: 022-26765506/26763179 mob: 9320261049
Email - expert@globalforensic.in