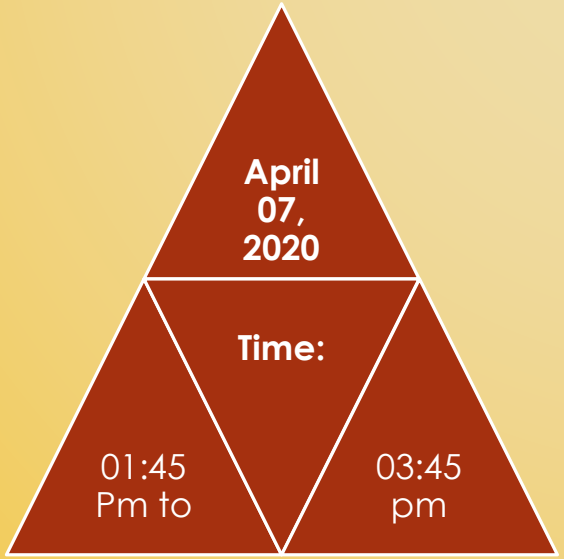
Webinar on Tools and Techniques of Forensic and System Audit- Opportunities for Professionals

Navjit Singh

Insolvency Professional Agency of Institute of Cost Accountants of India



Process of System & Forensic Audit

- Know the subject & Client (Stakeholder) Private, Public, Government: Statute, Agency, Regulator Global.
- Business Risk & Control- Internal Audit & (SOP) & External Prevention control.
- External Audit & Inspection Report:-(Opinion & fairness Audit, Report Review)-Historical Data & Present EDP System observation)-Threat & Vulnerability Test and Ethical Hacking.
- Scope, Timeline, Resources Analysis & Fee estimation(Preliminary Review & Planning).
- Engagement Letter (Scope, Time & Fee) & Management Representative letter (MRL & Third Party Arrangement).
- SWOT & Pestel Analysis (Industry & Competitor & Auxiliary contract clause) & other theory (Model-Techniques analysis and formula devices)-Simulation, Forecasting, Ratio Analysis Results & Norms.
- Organization Structure-Polices & Strategy (Vision & Mission).
- Management Records & System Configuration(In Features)-Lan/Internet/Cloud.

Process of System & Forensic Audit

- Resources & Infrastructure (Allocation of Resources & Team)-Execution Plan.
- Records, Documents, Mgt Data & EDP System (Data Warehouse, Management software & Package).
- Selection of Tools & Techniques for System & Forensic Audit for-(Detention Control).
- Data, System & Pattern Analysis (Testing, Approach & Analysis Tools)-Execution.
- Compliance & Substantive Test (Implementation).
- Observation, Interview & Group Discussion.
- Detention of Red flags & Controllable Transaction (Arms length Transaction or Fabricated Devices Identification).
- Further Investigation through Advance Excel/Data Mining Tools/Techniques (Digital Forensic).
- Data Mining, Capture, Storage, Revival Tools Selection (Prevention, Storage & Revival Devices)- BCP/DRP/(Black/White/Gray-Box, Alternate Mirror/ Arrangement, Site, Cloud/ Devices.

Process of System & Forensic Audit

- Preliminary Report & Discussion with Top Management (Client).
- Interrogation & Identification of Modus of Fraud (BCP/DRP)-Shortcoming & Pinpoint.
- Stage wise Final Conclusive Report-Presentation & its contents (Drafting-Limitation & Liability).
- Loss Impact & Allegation (Accused Disclosure).
- Pledging & Court Trial (Course of action) or Conclusion(Reference & Exit)
- Recommendation & Corrective Measures (Action)-(Separate Assignment)
- Continuous Prevention Control (Due Diligence & Upgradation)
- Challenge & Opportunity (Competition & Networking)-Advisor/Retain Ship.
- Continuous Professional Knowledge (Knowledge Bank-KPO-Consultancy concern)
- Global Technology & Resources (ISACA/Institute Course/International body Membership & Association-Team Continuous Upgradation-Live Google Data/Devices/Website).

Accounting & Accounting Types

- Accounting policies are the specific principles and procedures implemented by a company's management team that are used to prepare its financial statements. These include any accounting methods, measurement systems, and procedures for presenting disclosures.
- The types of Accounting.
- Financial Accounting. This field is concerned with the aggregation of financial information into External Reports.
- Public Accounting.
- Government Accounting.
- Statutory Accounting.
- Management Accounting.
- Tax Accounting.
- Cloud, HRA, Block Chain, SAP Accounting & other Statues Accounting (Report/Forms/Documents (Online-Manual)).

Hardware & Software System

- The various **examples** of **Hardware Devices** in the **Computer(EDP SYSTEM & DATA-ENVIRONMENT-DEVICES)** are output devices like printer, monitor, input devices like keyboard, mouse. **Hardware** also includes internal components like motherboard, RAM, CPU and secondary storage devices like CD, DVD, hard disk, etc.
- Sometimes abbreviated as **SW** and **S/W**, **Software** is a collection of instructions that enable the user to interact with a computer, its hardware, or perform tasks. Without software, most computers would be useless. For example, without your Internet browser software, you could not surf the Internet or read this page. Without an operating system, the browser could not run on your computer. The picture shows a Microsoft Excel box, an example of a spreadsheet software program. MS Word, WordPad and Notepad.
- ERP, SAP, SPECIALLANGAUGE, ORACLE, SPECIFIC DESIGN, TALLY, BLOCK CHAIN, ARTIFICAL INTELLIGIENCE, DIGITAL, ROBOTICS SOFTWARE.
- Internet browsers like Firefox, Safari, and Chrome, Microsoft Power Point, Keynotes, Auto CAD, MySQL, Oracle, MS Access, Apple Numbers, Microsoft Excel, Real Player, Media Player.

What is Internal Control & Auditing

- **The Seven internal control procedures are separation of duties, access controls, physical audits, standardized documentation, trial balances, periodic reconciliations, and approval authority.**
- Separation of Duties.
- Accounting System Access **Controls**.
- Physical Audits of Assets.
- Standardized **Financial** Documentation.
- **Auditing is the systematic examination of the books of accounts and the other documents of the company which is conducted with the main objective of knowing that whether the financial statement prepared and presented by the company shows a true and fair view of the organizations.**
- **Inspection & Due Diligence:- most of these are for Compliance & management SOP policies objectives.**
- **Internal Audit and various other audit:- Management, Financial, Secretarial, Committee Formation Report, Statutory.**

Software System / Control Device

- **Internet** is the term given for public network infrastructure. Thus while **Cloud** refers to remote computing resources, **Internet** mean the public communication infrastructure and its associated protocols that help computing devices connect globally. **Internet** is a way that provides connectivity to the **Cloud**.
- A **software firewall** will **protect** your computer from outside attempts to control or gain access your computer. For example, Windows **Firewall** is a Microsoft Windows application that notifies users of any suspicious activity. The app can detect and block viruses, worms, and hackers from harmful activity.
- There are three main **cloud computing types**, with additional ones evolving—software-as-a-service (SaaS) for web-based applications, infrastructure-as-a-service (IaaS) for Internet-based access to storage and **computing** power, and platform-as-a-service (PaaS) that gives developers the tools to build and host Web
- **The five types of firewall are:**
- **Packet filtering firewall**, **Circuit-level Gateway**, **Stateful inspection firewall**, Application-level gateway (aka proxy firewall),Next-generation firewall (NGFW).

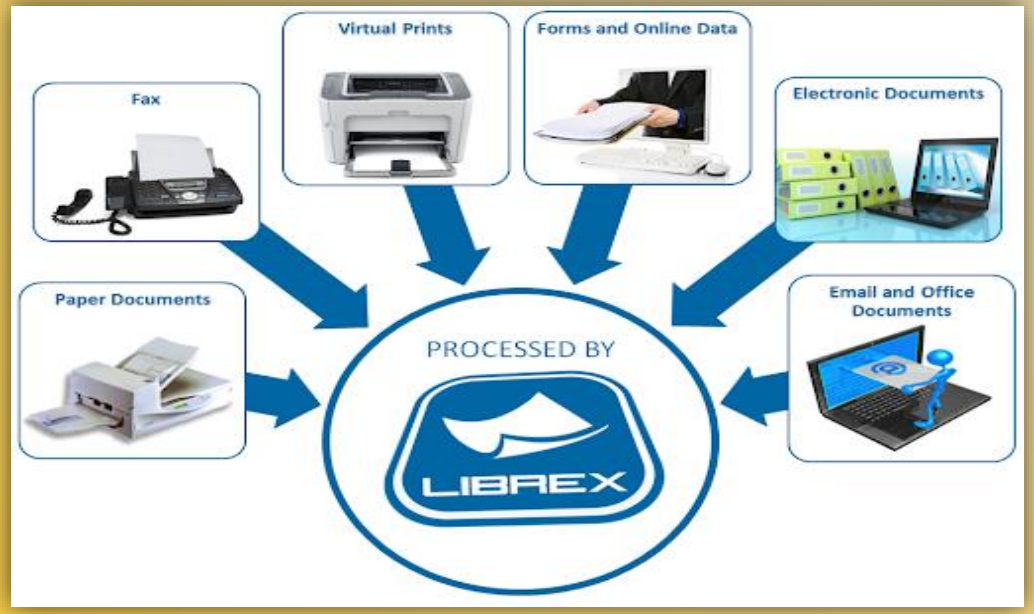
Software System / Control Device

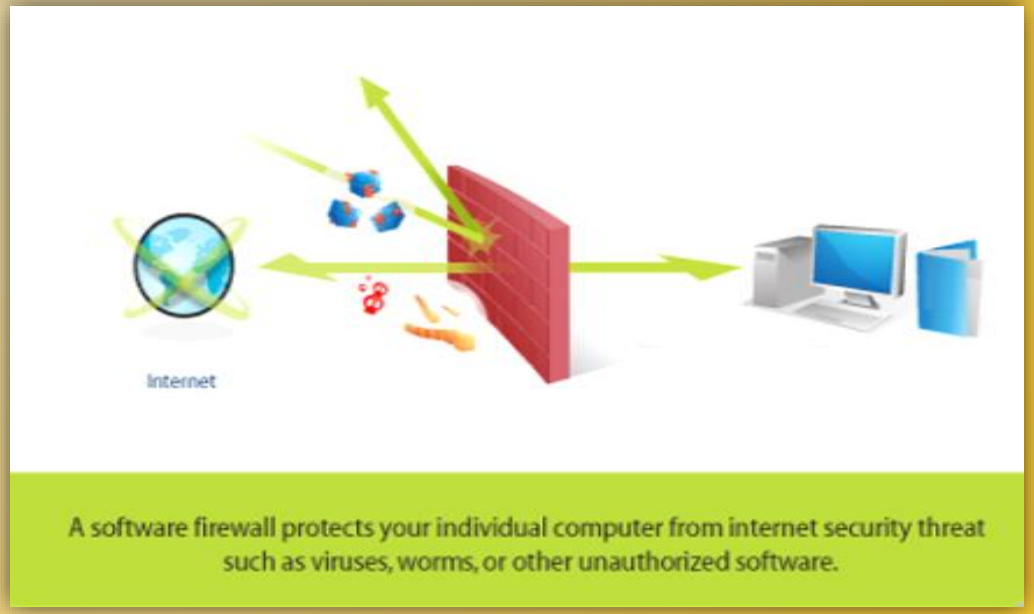
- **High-quality device control software:**

  Provides visibility into who is using what **devices** on which endpoints.

- **Controls how these devices are being used to ensure only legitimate business use.**

  Ensures that data transferred onto these **devices** is encrypted to prevent unauthorized use or dissemination.





Difference System & Forensic Audit

- A **Forensic Audit**/ Examination is designed to focus on reconstructing past financial transactions for a specific purpose, such as concerns of fraud, whereas an internal **audit** is typically focused more on compliance and/or the performance of the organization.
- An **Information System (IS) Audit** or **information** technology(IT) **audit** is an examination of the controls within an entity's **Information** technology infrastructure. An evaluation of internal controls may or may not take place in an IS **audit**. Reliance on internal controls is a unique characteristic of a Financial **Audit**.

Figure 5. The Linear Representation of the Fraud Management Lifecycle Theory.

A more realistic representation of the Fraud Management Lifecycle includes not only the flow of activities from the front end (deterrence & prevention) to the back end (investigation & prosecution), but the interactions and interrelationships between each of the various lifecycle stages. The completely interconnected nodes of a Fraud Management Network are pictured in Figure 6. The linear front end to back end process is facilitated by the flow of information around the exterior of the network, while the interactions and interrelationships between the stages are represented by the connections through the center of the network.

Techniques of Management internal Check Control (IFC)-SOP / Staregy / In Built Devices

- **Ethical Hacking** and **ethical hacker are** terms used to describe **hacking** performed by a company or individual to help identify potential threats on a computer or network. An **ethical hacker** attempts to bypass system security and search for any weak points that could be exploited by malicious **hackers.**
- **Penetration Testing**
- Capgemini conducts a full suite of technical testing to validate the effectiveness of controls and determine the integrity or configuration of a network, system, or application. Capgemini is experienced in conducting testing within critical operational environments, heavily regulated industries, and on a wide variety of devices and systems. Our testers will partner with you to understand your needs and objectives, whether they are driven by compliance and regulations or simply a desire to be as secure as possible, and then build the appropriate test scenarios. Through our rigorous adherence to the predefined “Rules of Engagement”, we will ensure there are no impacts to your operations or business. Based on the findings of our assessment and testing, we make recommendations for specific mitigations to reduce risks and prevent incidents in an organization’s business and operational environment.

Techniques of Management internal Check Control (IFC)-SOP / Staregy / In Built Devices

- Red Teaming and Threat Simulation:- Password Authentication, Camera, Odd Events Control, Validation Tools.
- **Well Architected Networks**, effective controls, and secure configurations are all important contributing factors to your cybersecurity posture. However, without the proper visibility, skillsets, and processes your capabilities are incomplete. Capgemini's Red Teaming and Threat Simulations will assess how your people, processes, and technology are working together to actively defend your enterprise. These solutions will enable you to better understand your detection, response, and analysis capabilities, and highlight tactical and strategic mitigation opportunities to ensure more effective defense in depth across the entire threat spectrum. Our Capgemini testers will work with you to understand your threat profile, identify areas of concern and interest, and partner with you to establish a series of engagements and interactive scenarios designed to confirm your capabilities are operating as intended and then push your organization to the limit. The result will be educational for both you and your team, providing actionable insights and observations to improve your overall security posture.

System BCP/DRP Control Testing

- Essentially, the **DR Plan** is a part of the bigger **BCP**. The **BCP** consists of a business impact analysis, risk assessment and an overall **business continuity** strategy; while the **DR plan** includes evaluating all backups and ensuring any redundant equipment critical to recovery is up-to-date and working**.**
- **5 Types of Antivirus Programs.**
- AVG. AVG is one of the most popular **antivirus** programs that can be obtained for free, and it's easy to download directly from the internet.
- McAfee.
- Norton.
- Kaspersky.
- Ad-Aware.

Types of System and Forensic Fraud Motive

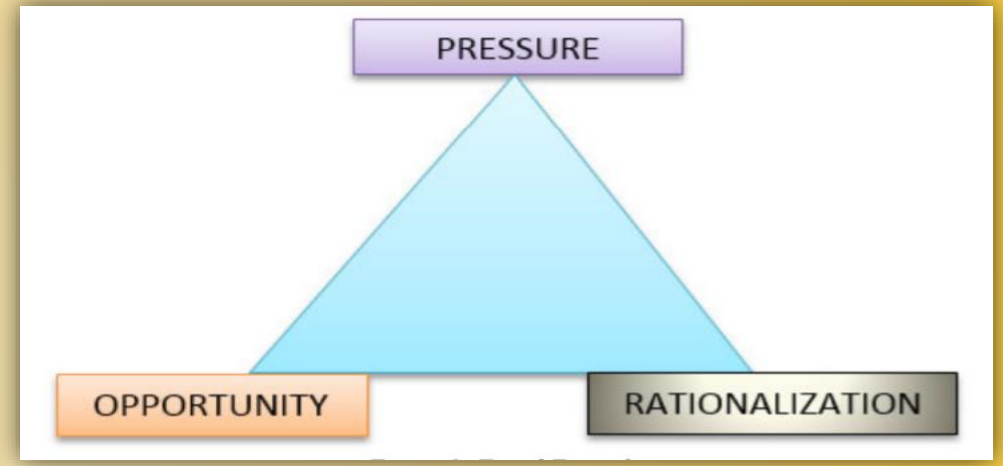
- **Corruption** There are three types of corruption fraud: conflicts of interest, bribery, and extortion. Research shows that corruption is involved in around one third of all frauds. n In a conflict of interest fraud, the fraudster exerts their influence to achieve a personal gain which detrimentally affects the company. The fraudster may not benefit financially, but rather receives an undisclosed personal benefit as a result of the situation. For example, a manager may approve the expenses of an employee who is also a personal friend in order to maintain that friendship, even if the expenses are inaccurate. n Bribery is when money (or something else of value) is offered in order to influence a situation. n Extortion is the opposite of bribery, and happens when money is demanded (rather than offered) in order to secure a particular outcome.
- **Asset Misappropriation** By far the most common frauds are those involving asset misappropriation, and there are many different types of fraud which fall into this category. The common feature is the theft of cash or other assets from the company, for example: n Cash theft – the stealing of physical cash, for example petty cash, from the premises of a company. n Fraudulent disbursements – company funds being used to make fraudulent payments. Common examples include billing schemes, where payments are made to a fictitious supplier, and payroll schemes, where payments are made to fictitious employees (often known as ‘ghost employees’). n Inventory frauds – the theft of inventory from the company. n Misuse of assets – employees using company assets for their own personal interest.

Types of System and Forensic Fraud Motive

- **Asset Misappropriation** By far the most common frauds are those involving asset misappropriation, and there are many different types of fraud which fall into this category. The common feature is the theft of cash or other assets from the company, for example: n Cash theft – the stealing of physical cash, for example petty cash, from the premises of a company. n Fraudulent disbursements – company funds being used to make fraudulent payments. Common examples include billing schemes, where payments are made to a fictitious supplier, and payroll schemes, where payments are made to fictitious employees (often known as 'ghost employees'). n Inventory frauds – the theft of inventory from the company. n Misuse of assets – employees using company assets for their own personal interest.
- **Financial Statement Fraud** This is also known as fraudulent financial reporting, and is a type of fraud that causes a material misstatement in the financial statements. It can include deliberate falsification of accounting records; omission of transactions, balances or disclosures from the financial statements; or the misapplication of financial reporting standards. This is often carried out with the intention of presenting the financial statements with a particular bias, for example concealing liabilities in order to improve any analysis of liquidity and gearing.

Green Flags

- **GREEN FLAGS** are symptoms or indicators of fraud, white collar crime or something detrimental to the interest of the organization. To the contrary there are other signals which could also imply the existence of fraud but do not activate alarm bells. Rather they may even lead to a greater sense of assurance and comfort in a scenario which may be potentially infused with fraud. These signals are referred as ‘green flags’. The instance of Green Flags could be helpful in identifying are unusual signs or inconsistencies, but apparently harmless or perhaps even helpful.
- **Triangle & Diamond Analysis**



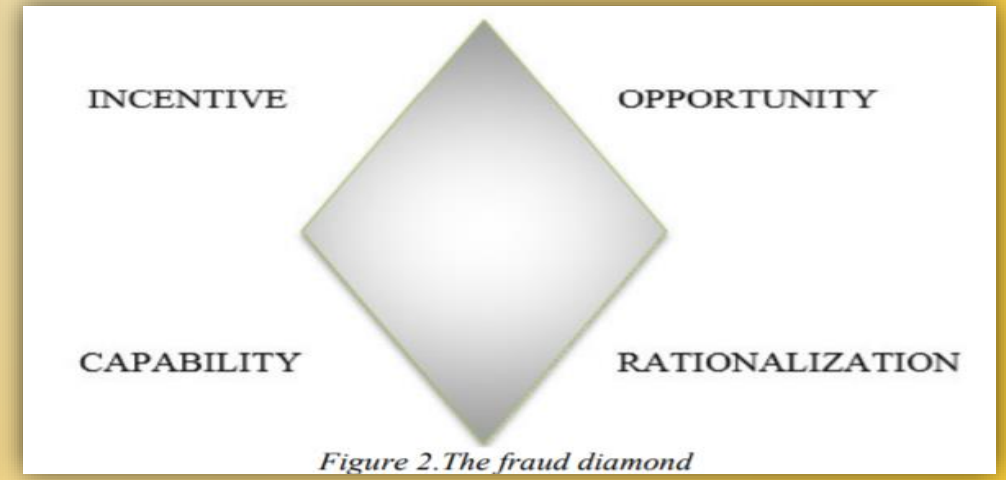


Figure 2.The fraud diamond

Red Flag for SYSTEM & Forensic Audit :-Red Flags are nothing but symptoms or indicator of situation of fraud (liiustration)

- **Common Types of Red Flags:** The most common types of Red Flags and fraudulent activity can be categorized as:
  - **Employee Red Flags**
  - **Management Red Flags**
- **Employee Red Flags are like:**
  - **Employee lifestyle changes: expensive cars, jewelry, homes, clothes, Significant personal debt and credit problems ,Behavioral changes: these may be an indication of drugs, alcohol, gambling, or just fear of losing the job ,High employee turnover, especially in those areas which are more vulnerable to fraud ,Refusal to take vacation or sick leave and Lack of segregation of duties in the vulnerable area.**

Management / Organization/Data Red Flags

- **Management Red Flags:-**

- are like Reluctance to provide information to auditors, Managers engage in frequent disputes with auditors, Management decisions are dominated by an individual or small group, Managers display significant disrespect for regulatory bodies, There is a weak internal control environment, Accounting personnel are lax or inexperienced in their duties Decentralization without adequate monitoring, Excessive number of checking(identical code/figures accounts, Significant downsizing in a healthy market, Continuous rollover of loans, Excessive number of year end transactions, High employee turnover rate, Unexpected overdrafts or declines in cash & cash equivalent balances, Refusal by company or division to use serial numbered documents (receipts), Compensation program that is out of proportion, Any financial transaction that doesn't make sense - either common or business, Service Contracts result in no, Photocopied or missing documents, Frequent changes in banking accounts, Frequent changes in external auditors, Company assets sold under market value.

CAAT & IDEA Data Mining Tools (Big Data /Volume /various Forms/ Language)

- **Computer Assisted Audit Techniques** (**CAATs**) **is** the tool which **is used** by the auditors. This tool facilitates them to make search from the irregularities from the given data. With the help of this tool, the internal accounting department of any firm **will** be able to provide more analytical results.
- **IDEA Software**, often referred to as **IDEA** management **software**, is a powerful solution that you can use to ask for, collect, analyze, and track **IDEAS** from diverse groups of people, also called a "crowd." For businesses, this typically means employees, but many companies also use it to solicit and vet new **IDEAS** from their.

Tool	Strengths	Weaknesses
Support Vector Machine and Stylometry Used to determine authorship of e-mails [12]	• Based on Structural Minimisation principle • Provides a systematic way of determining the relative effectiveness of raw style markers	• Does not yield admissible evidence • More experimentation to determine sensitivity of authors to style markers
Writing-Style Features and Classification Techniques Used to address of online messages and said author [42]	• Experimental approach able to identify author • Structutral and content specific features allow identification of authors • Uses 3 classification techniques • Applied to multiple languages: English and chinese	• Identification of optimal set of features for online messages • More experimentation needed • Validation of proposed technique in the field
Integrated E-mail forensic analysis framework Java based application used to determine authorship of e-mails [20]	• Theoretical foundation based on statistical analysis, text mining and stylometry together with social networking techniques • E-mail geographic localisation – used to localise information relating to suspect e.g. e-mail server	• Level of cohesion of techniques needs to be increased in order to obtain more credible results • Further investigation is prompted for e-mail social networks
AutoMiner Noval data mining technique using frequent patterns and comparing it to write print of an individual [22]	• Unique identifier for authorship identification – namely write print which is dynamically extracted • Accuracy of 86 – 90% • Robust method for determining authorship	• As minimum supported threshold of intervals (features) increase, the accuracy decreases • Manual examination of write prints as many frequent patterns are not obvious
EnCase Enterprise Edition 4.19a designed to integrate with enterprise security architecture, providing enhanced access control and audit functions, and enabling digital investigators to process many systems on a network simultaneously. [10]	• Tool of choice for enterprise investigations • Extracts more data than PDIR • Does not alter data on remote system • Uses System calles SAFE to manage security • Data acquisition of 3.5 MB/s • Gives information about which files are opened • Can integrate with intrusion detction systems	• Data acquisition slow due to SAFE system initailly reading device • Require administrator privalages • Cannot view data on network shares limiting amount of data • Provide most information possible
ProDiscover IR 3.5 designed to examine one system at a time and is useful for focused investigations involving a small number of computers. [10]	• Alters last accessed date/time stamps when performing some processes • Has optional encryption and password protection • Only presents information that is verifiably complete	• Has optional encryption and password protection not enabled by default for servlet • Data acquisition of 5.5MB/s • Require administrator privlages • Cannot view data on network shares limiting amount of data

Data Mining Tools (Others)

List of Most Popular Data Mining Tools & Applications

- Rapid Miner
- Orange.
- Weka.
- KNIME.
- Sisense.
- Apache Mahout.
- Oracle **Data Mining**.
- Data Melt.
- Advance Excel
- IDEA
- CAAT

- **Digital Forensic** examinations use **computer**-generated data as their source.
- **Best System & Forensic Tools that are promising for today's computers:**
- SANS SIFT.
- Pro Discover Forensic.
- Volatility Framework.
- The Sleuth Kit (+Autopsy)
- CAINE.
- Xplico.
- X-Ways Forensics.
- hat are digital forensic tools?
- LoadRunner & Success Factors.

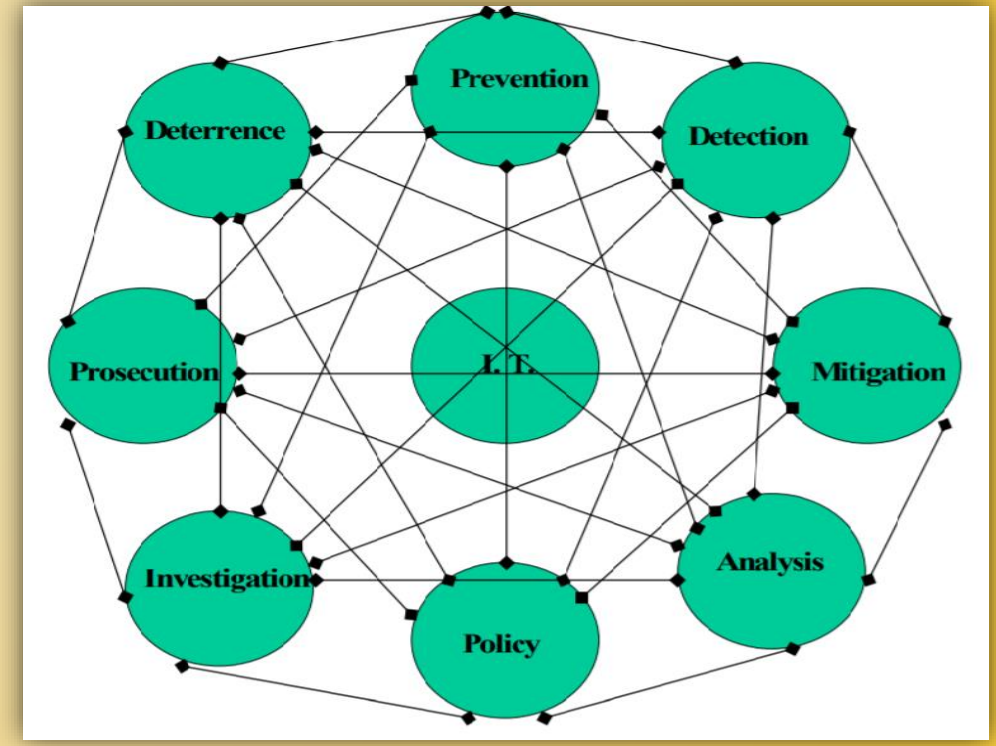
Advance Excel Tools (Formula Analysis)

- **Advanced Excel Formula and Functions**
- VLOOKUP. The function is used to look up for a piece of information in a large segment of data and pull that data to your newly formed table.
- Sum Function.
- MAX MIN function.
- IF Function.
- SUMIF Function.
- COUNTIF Function.
- AND Function.
- OR function.

- Consolidation Data from Different Text Files.
- Features and Functions of Microsoft Excel for Standardization of Data.
- Use of Sorting and Pivot Table in the Given Data.
- Functions of Pivot Table in Microsoft Excel to analyze transactions What learn?.
- Consolidate data from different text files using the Text Import Wizard and Fill Series.
- Features and Consolidation Data from Different Text Files Features.

Advance Excel Tools (Formula Analysis)

- Functions of Microsoft Excel for Standardization of Data and Standardize data of the Excel Sheet by using Remove Duplicate Entries, Sort Data.
- Check Consistency, VLOOKUP Function and If NA/If Error. *
- Use of Sorting and Pivot Table in the Given Data and Functions of Pivot Table in Microsoft Excel to analyze Transaction.

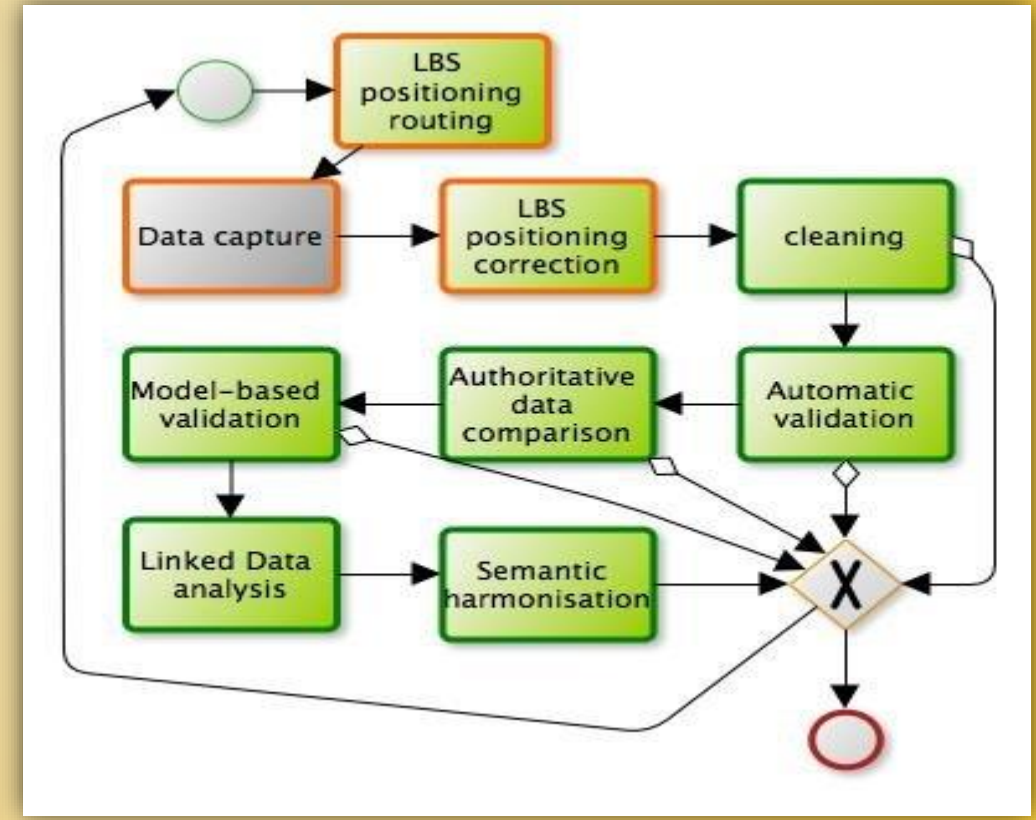


Data Capturing Methods/ Tools

- Multiple methods are available for capturing data from unstructured documents (letters, invoices, email, fax, forms etc)The list of methods identified below is not exhaustive but it is a guide of the appropriate usage of each method when addressing business process automation projects.
- As well as considering the method of data capture, due consideration of the origins of the documents(s) that need to be captured must happen, to see if the documents are available in their original electronic format which, has the potential to massively increase data capture accuracy and remove the need for printing and scanning. Methods of capture from documents in electronic format are identified below.
- Whenever a method of capture is considered, it is advisable in the first instance to consider the original documents, to determine if the document or form can be updated to improve the capture/recognition process and method. Investigation of the existing line of business systems, to determine what additional metadata can be extracted for free using a single reference, can provide significant advantages!
- The correct method(s) of metadata capture for a particular business process automation project, will consider all the methods identified below and the use of one or a number may be appropriate.

Data Capturing Methods/ Tools

- Data Duplication and Digital capturing Tools(Various tools can be found out from google sites)-costly/ customized/standard/accept in court of law and need and data detecting and data package norms).



Methods of Interrogation & Investigation

- **ArtimetrixAnalysis:Regression,Coefficient,Corerelation,Mean,Mode,Standarddeviation, Table,Graph,DiagramSimulation,Forecasting,Formula,Range,RandomNumber,Comparsion, Variable,Norms,Standard,Factor,Series,Probality**
- **Analytical Procedures** – Used to compare trends over a certain time period or to get comparative data from different segments
- **Computer-Assisted Audit Techniques** – Computer software programs that can be used to identify fraud , Forensic Investigation and Forensic Audit Methodology in a Computerized Work. (EXCEL, TALLY, IDEA, ERP Package Etc.)
- **Understanding Internal Controls and Testing** them so as to understand the loopholes which allowed the fraud to be perpetrated.
- **Methods of Investigations** Common techniques used for collecting evidence in a forensic audit include the following:
- 1. Substantive Techniques – For example, doing a reconciliation, review of documents, etc.

Methods of Interogation & Investigation

- Interviewing and Interrogation- Interview and Interrogation are two major techniques in investigation. That are used to elicit responses from the suspect or accused. It should however be noted that the investigator (interviewer or interrogator) cannot usurp the power of the court of competent jurisdiction by pronouncing the suspect or accused guilty. His/her role is to gather evidence that can be used to prove or disprove the act in issue.

What is System Forensic Audit-Drafting & Pledging

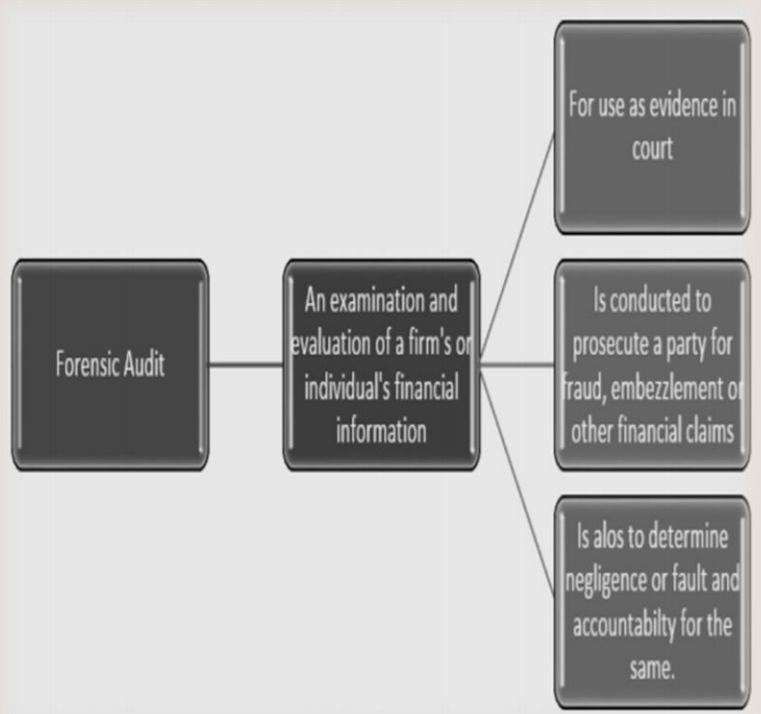
- **Drafting** refers to the writing of Legal Documents.
- **Pleading** refers to a legal document filed **in a** lawsuit. This can be a document pertaining to the initiation of litigation or a document in response to this initiation. Conveyancing refers to the transferring of a real property to its new owner by means of deeds.
- **Trial** (Legal Course Action): Judgement, Order (Settlement, Damage, Penalty, Imprisonment).

What Steps & Procedure of Forensic Audit

- **How Is System & Forensic Auditing Investigation Conducted?**
- Step #1: Accept the investigation.
- Step #2: Determine the categories of the investigation.
- Step #3: Plan the investigation.
- Step #4: Gather the evidence.
- Step #5: Report of the findings.
- Step #6. The investigation process.
- Step #7: Court proceedings.

System & Forensic Audit Trail Procedure

- ONE: Begin the case (Respond to Complaint, etc.) .
- TWO: Evaluate the allegations or suspicions.
- THREE: Conduct due diligence background checks.
- FOUR: Complete the internal stage of the investigation.
- FIVE: Check for predication and get organized.
- SIX: Begin the external investigation.
- SEVEN: Prove Illicit Payments.
- EIGHT: Obtain the cooperation of an inside witness.
- NINE: Interview the primary subject.
- LASTLY: Prepare the Final Report.

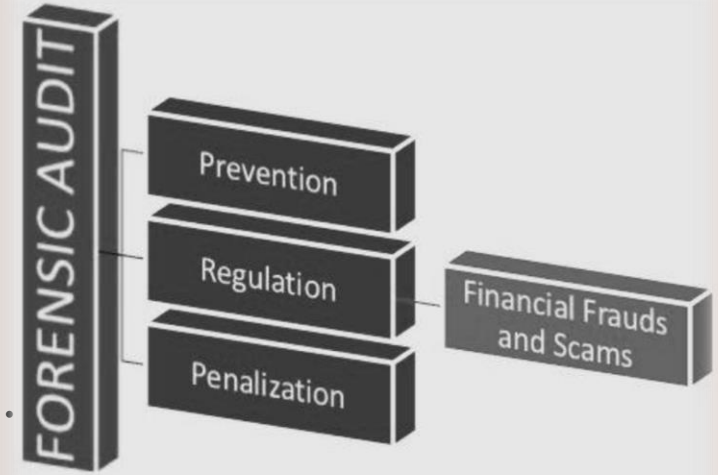


Systems & Forensic Audit Report-Contents

1. Index
2. Overview
3. Executive summary
    I. Facts in brief
    II. Methodology in brief
    III. Findings
4. Background and Allegations
5. Detailed Methodology
6. Main Report
7. Detailed Time-line
8. Scope Reconciliation
9. Detailed methodology- collection of evidence and implementation
10. Procedure Performed
11. Findings in detail-point wise finding and analysis
12. Limitations
13. Disclaimers & Liability Clause
14. Glossary and Abbreviations
15. Appendices and Exhibits

System & Forensics Courses Audit Report-Contents

- It is an institute offering corporate, legal, **forensic** science and **cyber forensics with system configuration control events finding** courses in
- DISA/CISA.
- **Indian** School of Ethical Hacking.
- Gujarat **Forensic** Sciences University.
- SRM University.
- IIIT Delhi (Indraprastha Institute of Information Technology).
- ISACA-COBIT/COSO etc.
- Networking, Artificial Intelligence, Block Chain, ERP, Language, Accounting & Software and Robotics software utility knowledge, training Courses.



Question & Answer Session:-

From:.

Navjit Singh

{FCMA, FCA, Insolvency Professional, LLB, DISA(ICAI),
Diploma in Business Valuation(ICAI),
Certification Course: Concurrent Bank Audit, Anti Money laundering Laws,
***Forensic Accounting and Fraud Prevention**, Service Tax (ICAI)}*

Navjit92ca@gmail.com & 9311162970, 9999240273