Fraud Detecting Techniques

Lesson 15

KEY CONCEPTS

■ Fraud ■ Investigation ■ Detection ■ Know Your Customer (KYC) ■ Misconduct ■ Digital Evidence ■ Clustering ■ Decision Tree

Learning Objectives

To understand:

- The meaning of Fraud, Investigation and Detection
- Early warning indicators of Fraud such as Unusual Financial Activity, Poor Accounting, Unusual behavior, Unexplained Inventory, Employee Turnover, Weak or lack of Internal Controls, Complaints or Tip, Weaknesses in IT Security, Suspicious Emails or Messages
- The term 'Money Laundering'
- Techniques used for Fraud Detection in Money Laundering
- Fraud Detection using General Audit Techniques such as Analytical procedures, Inquiry, Observation, Re-performance, Sampling, Inspection etc.
- Statistical and Mathematical Techniques in Fraud Detection
- Technology based Fraud Detection Techniques
- Data Mining Techniques for Fraud Detection

Lesson Outline

BACKGROUND TO FRAUD DETECTING TECHNIQUES

"There is enough in this world for every man's need, but there is not enough for every man's greed" – Mahatma Gandhi.

One of the major reason for frauds across the globe that is perpetrated by individuals or by an organisation is greed.

Meaning of Fraud: Wrongful or criminal deception intended to result in financial or personal gain.

Meaning of Investigation: The action of investigating something or someone; formal or systematic examination or research.

Meaning of Detection: The action or process of identifying the presence of something concealed.

Fraud investigation is a critical tool for protecting individuals and organisations from financial losses and ensuring that those who engage in fraudulent behavior are held accountable for their actions.

Fraud detection is a critical component of risk management for individuals and organisations. By employing effective fraud detection strategies, individuals and organisations can minimise their exposure to financial losses and reputational damage caused by fraud, while also promoting greater trust and security in their interactions with others.

As per Association of Certified Fraud Examiners (ACFE), Detection is an essential step in fraud investigation because the speed with which fraud is detected can have a substantial impact on the magnitude of fraud.

Fraud can take many forms and can be perpetrated by individuals or groups with various motivations. Common types of fraud include identity theft, credit card fraud, insurance fraud, and investment scams, among others. Fraudsters may use various tactics, such as impersonation, phishing, hacking, or social engineering, to gain access to sensitive information or manipulate victims into providing financial resources.

The Association of Certified Fraud Examiner's 2022 Report to the Nations time and again demonstrates that 42% of Fraud is detected only by way of Tip and of this 55% of tip came from Employees, 18% from the customers, Anonymous 16%. Fraud losses were 2X higher at organisations without hotlines. 45% of cases detected by tip with training within a period of 12 months with hotlines.

What is fraud detection?

Fraud detection is the process of identifying and preventing fraudulent activity in various contexts, including financial transactions, online interactions, insurance claims, and more. It is an important tool for individuals and organizations to protect themselves against financial losses and reputational damage caused by fraud. It is a postmortem after the alleged fraud has happened and a reactive action.

As seen above fraud can take many forms and it can be perpetrated by individuals or groups with various motivations. Common types of fraud include identity theft, credit card fraud, insurance fraud, and investment scams, among others. Fraudsters may use various tactics, such as impersonation, phishing, hacking, or social engineering, to gain access to sensitive information or manipulate victims into providing financial resources.

To effectively detect and prevent fraud, individuals and organizations must employ a range of strategies and tools. These may include automated systems for monitoring financial transactions, implementing secure authentication protocols, conducting background checks on individuals or organizations, and maintaining robust cybersecurity practices.

Fraud detection also requires a deep understanding of human behavior and the ability to identify patterns or anomalies that may indicate fraudulent activity. This may involve analysing data and behavior over time, identifying changes in behavior or activity that deviate from normal patterns, and conducting investigations to determine the root cause of suspicious activity.

It should be noted that the information technology is growing at a rapid pace especially after the COVID-19 pandemic across the globe. Company Secretaries in Industry or in Practice or as a Forensic Auditor cannot be an expert in all emerging technologies. Hence, the fraud detection tools discussed in this study lesson are very dynamic. What is relevant today may become obsolete tomorrow. Further, it involves working along with Data Scientists, Computer Scientists, Artificial Intelligence Researchers, Blockchain Developers and so forth.

EARLY WARNING INDICATORS OF FRAUD

1. **Unusual Financial Activity**

   This may include unexplained transactions, changes in account balances, or unexpected cash flow patterns, unexplained losses, increased expenses and/or decreased revenues.

2. **Poor Accounting or inconsistent or Missing Documentation**

   If financial records are incomplete, missing, or do not match up with other records, any accounting or record-keeping irregularities, such as missing documents, unexplained balances, or unrecorded transactions this could be a red flag for fraud.

3. **Unusual behavior or Changes in behavior or lifestyle by Employees**

   This could include employees who suddenly start working unusual hours, show signs of financial stress, or exhibit other unusual behaviors. Keep an eye or understand from interviewing with key persons if they observed any sudden changes in behavior or lifestyle of employees or stakeholders. For example, if an employee suddenly starts buying expensive items, it could be a red flag.

As per ACFE 2022 report 85% of all fraudsters displayed at least one behavioral red flag: 39% (Living beyond means), 25% (Financial difficulties), and 20% (unusual close relationship with vendors), and 13% (unwillingness to share duties).

4. **Unexplained Inventory or Movable Assets Shortages**

   If inventory levels or movable assets are lower than expected or if there is a discrepancy between inventory levels, movable assets and its records, this could be a sign of fraud. Stealing of inventory happens in industry in trading and manufacturing of consumer goods like high value mobile phones, tablets, laptops etc.

5. **Employee Turnover**

   High employee turnover, particularly in key financial roles, could be a sign of fraudulent activity which needs to be carefully probed.

6. **Weak or lack of Internal Controls**

   If an organisation has weak internal controls, this could make it easier for fraud to occur. Be aware of any instances where there is a lack of internal controls or segregation of duties, which could make it easier for fraud to occur.

7. **Complaints or Tip**

   If employees, customers, or vendors report suspicious activity, this should be taken seriously and investigated since majority of frauds are detected based on Complaints or tip and not by an internal audit or external audit.

8. **Weaknesses in IT Security**

   Any weaknesses in IT security that could allow unauthorised access to sensitive data or transactions. Many entities in addition to financial audit also do audit of their systems and network with the help of Vulnerability assessment and Penetration testing (VAPT).

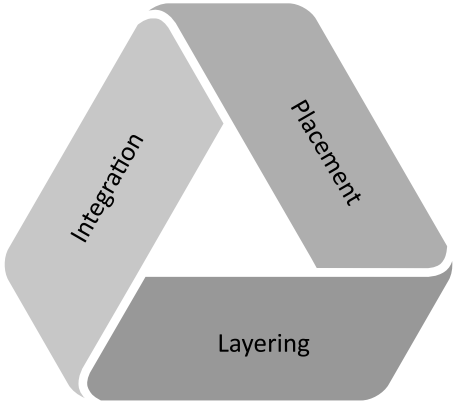
9. **Suspicious Emails or Messages**

   If employees receive emails or messages that appear to be from a legitimate company or organisation, but are asked to click on a link or provide additional information, it could be a phishing scam designed to steal entity's information.

   By monitoring these early warning indicators and implementing strong internal controls, organisations can help prevent fraud and minimize its impact if it does occur.

MONEY LAUNDERING AND ITS DETECTION

Money laundering starts with proceeds from a specific source. For a variety of reasons the launderer wants to hide the money trail. Money laundering takes place in three distinct stages: Placement, Layering and Integration. The money launderers including drug dealers, fraudsters, tax evaders and terrorists have many challenges when moving money through each of the stage.



Placement: The placement of funds of illegal proceeds into a financial institution is the first stage of money laundering and it is not so easy to do. The challenge is mainly due to dealers deal in hard currency. Placing the cash into a financial system undetected is difficult because the banks are required to file a report with the Government for all cash deposits in excess of threshold limit. For example in the United States and Canada any cash deposits in excess of $ 10,000 is automatically picked up by the reporting system.

According to the new rules, PAN and Aadhaar will be required for depositing cash more than the threshold limit in a bank or post office in any one financial year.

A bank (both private and nationalized bank) has to furnish a Cash Transaction Report (CTR) to the Financial Intelligence Unit (FIU) every month "incorporating all transactions over 10 lakh or its equivalent in foreign currency or a series of integrally connected transactions that add up to more than 10 lakh or its equivalent in foreign currency."

The FIU is empowered to get the CTRs under the Prevention of Money Laundering Act (PMLA). There have been CTRs where numerous small transactions were undertaken without mentioning the PAN and when these are inter-linked with the help of data mining tools a big picture of possible tax evasion or money laundering emerges.

To avoid their cash deposits from being reported, the launderers use a technique known as "smurfing". Smurfs known as "mules" are individuals recruited to open bank account and deposit cash in amount smaller than threshold limits prescribed in their countries. But moving millions of dollars or rupees can be a time consuming process and such suspicious movement of funds are also tracked by bank's software.

Hence, money launderer often purchase business that deal in cash like restaurants, bars, night clubs, malls, cinema theatre etc. and comingle their illegal proceeds with the funds of their business.

Layering

Once the proceeds of crime have been successfully injected into the financial system, the next stage is layering transactions by moving the proceeds through various banks or financial transactions. Law firms specializing in creating off-shore accounts can be used to set up shell companies, trusts or a foundation to purchase assets internationally.

In the case of transnational criminal matter, Mutual Legal Assistance Treaty (MLAT) has to be used, if both the prosecutor's country of origin and the subject's country of origin have entered into an MLAT. If there is no MLAT in place, letters rogatory (letters of request) are used to facilitate communication. Letters rogatory is slower and cumbersome than MLAT.

Due to the time delay in getting MLAT and LR, an astute money launderer could swiftly move funds through a number of foreign jurisdictions, effectively preventing law enforcement from tracing the money.

Money laundering is a complex process involving the concealment of the proceeds of illegal activities by disguising them as legitimate funds. Fraud detection techniques can be used to identify suspicious activities that may be indicative of money laundering.

Integration

The last stage of money laundering is moving the layered money into an account that appears to be for a legitimate purpose. Funds can be moved into clean bank account with explanations such as consulting fee, loan, dividend via wire transfer from an overseas shell company's bank account.

Techniques used for Fraud Detection in Money Laundering

Some of the common techniques used for fraud detection in money laundering include:

1. **Transaction Monitoring**

   Transaction monitoring involves the continuous surveillance of financial transactions to detect and flag suspicious activities. This involves the use of automated software programs to track transactions in real-time, analyse patterns, and identify anomalies or unusual behavior. Transaction monitoring is an automated process used to identify and analyse transactions for any unusual or suspicious patterns. The system analyses data such as the amount, frequency, and destination of transactions to identify any red flags.

2. **Customer Due Diligence (CDD)**

   CDD is a process of identifying and verifying the identity of customers, including their source of funds and the purpose of their transactions. This can help identify potential money launderers and high-risk customers.

3. **Know Your Customer (KYC)**

   KYC is similar to CDD but focuses on building a more detailed understanding of customers by gathering information about their financial behavior, transaction history, and risk profile. KYC is a mandatory process for financial institutions to identify and verify the identity of their customers. KYC helps to prevent fraud by ensuring that the customer is legitimate and not involved in any illegal activities.

4. **Enhanced Due Diligence (EDD)**

   EDD is a more intensive form of CDD and KYC, typically used for high-risk customers or those with complex transactions. This involves a deeper investigation of the customer's financial activity, including the source of funds, the purpose of transactions, and the nature of the relationship with the financial institution.

5. **Risk-Based Approach (RBA)**

   RBA involves assessing the level of risk posed by a customer, transaction, or business and applying appropriate measures to mitigate that risk. This can help financial institutions prioritise their efforts and resources in identifying potential money laundering activities.

6. **Artificial Intelligence (AI) and Machine Learning (ML)**

   AI and machine learning algorithms can be used to analyse large volumes of data, identify patterns, and detect suspicious activities in real-time. This can help financial institutions stay ahead of money launderers and adapt to changing fraud patterns.

7. **Suspicious Activity Reporting (SAR)**

   Financial institutions should monitor customer accounts for any suspicious activity, such as sudden large deposits, unusual transactions, or multiple transactions to the same destination. This can help to detect potential money laundering activities.

   SAR is a process of reporting suspicious transactions to relevant authorities, such as law enforcement or regulatory bodies. This can help to identify and investigate potential money laundering activities and prevent further criminal activity.

8. **Link Analysis**

   Link analysis is very effective for identifying the indirect link. When conducting a money laundering probe, link analysis is useful to track the placement, layering and integration of money as it moves around unexpected sources. It helps to uncover indirect relationships including those that are connected through

maze of subsidiaries. It can also help to detect a shell company. The forensic auditor could link between varieties of entities that commonly share an address.

How to detect shell companies using link analysis

It has been observed that most of the money laundering involves use of shell companies for doing money laundering. Detection of it involves examining the relationships between entities and identifying suspicious patterns.

- **Identify the Key Entities**: The first step is to identify the key entities that have to be analysed. These could be companies, individuals, or any other relevant entities.
- **Collect Data**: Collect data on the identified entities from various sources, including public records, corporate filings, social media, and other online sources.
- **Build a Chart**: Build a chart representing the relationships between the entities.
- **Analyze the Chart**: Use link analysis techniques to identify suspicious patterns in the chart. Look for entities that are linked to multiple other entities or that have unusual patterns of connections.
- **Look for Red Flags:** Look for red flags that may indicate the presence of a shell company, such as a company with no employees or physical location, a company with a history of frequent name changes or ownership changes, or a company that is linked to other suspicious entities.
- I**nvestigate further:** If auditor identifies a suspicious entity, investigate further to gather more information and verify the findings. He may need to conduct additional research or consult with experts in the field to determine whether the entity is a shell company.
- **Risk Assessment**: Financial institutions should conduct a risk assessment of their customers and transactions to identify high-risk customers and transactions. This helps to allocate resources and prioritize investigations on high-risk transactions.
- **Watch list Screening:** Watch list screening involves comparing customer names against government and international watch lists of known criminals, terrorists, and politically exposed persons (PEPs). This helps to identify high-risk customers and transactions and prevent money laundering activities.
- **Data Analytics:** Financial institutions can use data analytics to identify patterns and trends in customer transactions, enabling them to identify potential money laundering activities.

Overall, fraud detection techniques in money laundering require a combination of technological solutions, human expertise, and regulatory frameworks to be effective in detecting and preventing criminal activities.

MISCONDUCT

Asset misappropriation is a fraudulent conduct (or misconduct). Data analysis helps to detect frauds especially in bigger organisation with many employees, customers, vendors and due to a large amount of data, manual forensic audit is impractical. Inserting Ghost or fictitious employees in the payroll register are those who does not actually work for the entity. Detecting fraudulent payments and siphoning off funds can be detected with data analysis to cover ghost employees.

Tests that can help unravel fictitious employees are:

1. Check whether multiple employees are using the same bank account
2. Employee using multiple bank accounts
3. Multiple employees have same home address

4. Employees still on the payroll even after resignation/dismissal/ retirement date
5. Head count analysis department wise.

With the help of IDEA DATA analysis software etc., test for employees with the same address can be made as a process of fraud detection.

FRAUD DETECTION USING GENERAL AUDIT TECHNIQUES

Fraud detection is an important objective of any audit be it internal audit or statutory audit or a cost audit. General audit techniques can also be used and is very helpful to identify potential fraud risks and to gather evidence of fraudulent activities.

The responsibilities of the external auditor as they relate to fraud detection are clearly defined in International Standard on Auditing (ISA-240), The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements.

"The auditor is responsible for maintaining professional skepticism throughout the audit, considering the potential for management override of controls, and recognizing the fact that audit procedures that are effective for detecting error may not be effective in detecting fraud. The requirements in this are designed to assist the auditor in identifying and assessing the risks of material misstatement due to fraud and in designing procedures to detect such misstatement"

Some of the general audit techniques that can be used by auditors to detect fraud include:

1. **Analytical procedures**

   This involves analysing financial data to identify trends or anomalies that may indicate fraud. For example, the auditor can compare financial ratios with industry benchmarks or prior periods to identify unusual changes in the company's financial performance.

2. **Inquiry**

   This involves asking questions of management and other employees to identify potential fraud risks and to gather information about the company's internal control systems. The auditor can ask about unusual transactions, discrepancies in records, or unusual behavior by employees.

3. **Observation**

   This involves physically observing the company's operations to identify potential fraud risks. For example, the auditor can observe how cash is collected and counted to identify any weaknesses in the company's movable assets handling procedures which are susceptible to fraud.

4. **Re-performance**

   This involves re-performing calculations or procedures performed by the client to ensure their accuracy. This can help the auditor identify errors or discrepancies that may indicate fraudulent activities.

5. **Sampling**

   This involves selecting a representative sample of transactions or data to test for accuracy and completeness. This can help the auditor identify unusual transactions or patterns of behavior that may indicate fraud.

6. **Inspection**

   This involves examining records and documents, such as invoices, receipts, contracts, and bank statements, to verify their accuracy and completeness. This can help the auditor identify fraudulent transactions or falsified documents.

   In addition to the above mentioned general audit techniques, auditors can also use specialised audit procedures to detect fraud, such as data analytics and forensic accounting techniques.

The key to effective fraud detection is to be vigilant, skeptical, and thorough in gathering and evaluating audit evidence.

STATISTICAL AND MATHEMATICAL TECHNIQUES IN FRAUD DETECTION

Statistical and mathematical techniques play a crucial role in fraud detection techniques, as they enable financial institutions to identify and analyze large volumes of data to detect potential fraud patterns.

Here are some commonly used statistical and mathematical techniques in fraud detection:

Benford's Law

Frank Benford in 1920's made an interesting observation while examining his logarithm book. He noticed that the first few pages of his logarithm book were more worn out than the other pages. His theory was scientists spend more time dealing with logs that begin with 1, 2 or 3 and with each succeeding first digit the time it was used was decreased.

This led to remarkable mathematical discovery. In a population of naturally occurring multi-digit numbers, the multi-digit numbers beginning with 1, 2 or 3 must appear more frequently than multi-digit numbers beginning with digits 4 to 9.Benford law cannot be applied for non-natural numbers like Employee ID numbers, telephone numbers which are designed systematically to convey information that restricts the natural nature of the number.

Benford's law provides that the distribution of the digit in multi-digit natural number is not random but it follows a pattern which can be predicted. The goal of a Benford's law is to identify fictitious numbers when creating false documentation or transactions to cover the tracks by fraudsters.

Benford's Law is a statistical tool used to detect potential fraud in financial statements or other numerical datasets. The law states that in many naturally occurring datasets, the leading digit is more likely to be a small number (e.g., 1, 2, or 3) than a large number (e.g., 8 or 9).

One application of Benford's Law is in detecting fraudulent journal entries or fraudulent financial transactions in the books of account.

Suppose a company's financial statements show that there were several large expenses recorded during a particular period. A forensic accountant or auditor could use Benford's Law to investigate whether the expenses were legitimate or if they were inflated or fraudulent.

To do this, they would first examine the leading digits of the journal entries and calculate the expected frequency of each digit according to Benford's Law. If the actual frequencies differ significantly from the expected frequencies, it could indicate that the numbers were manipulated or fabricated.

Example:

A company's financial statements it is suspected that there were few fictitious expenses recorded during the year, with the following amounts in INR:

22,500

10,750

8,650

14,200

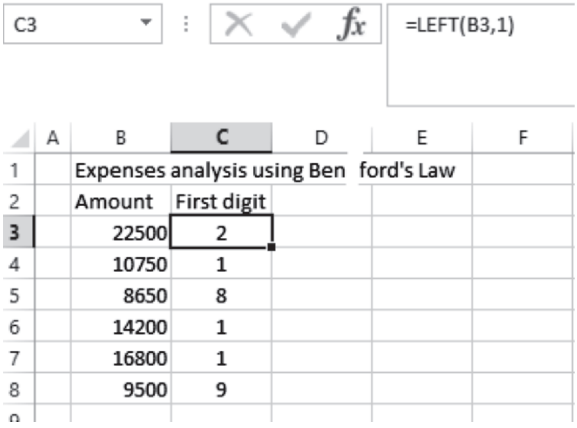
16,800

9,500

Using Benford's Law, forensic auditor would expect the following frequencies for the leading digit:

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

Extract the first digit from each number in column C using the LEFT function, and copied it down.

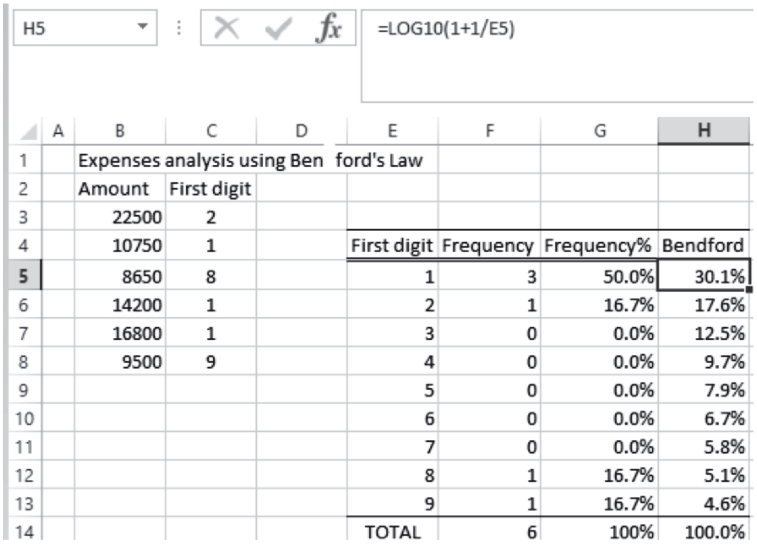


	A	B	C	D	E	F
1		Expenses analysis using Ben			ford's Law	
2		Amount	First digit			
3		22500	2			
4		10750	1			
5		8650	8			
6		14200	1			
7		16800	1			
8		9500	9			

Let's make a table and look at the frequency of each digit.

Use the COUNTIF function to count how many times each digit (1 through 9) occurs in column C and let's check our numbers against Benford's law.

The Excel formula for Benford's Law is =LOG10(1+1/d), where **d** is the leading digit:



	A	B	C	D	E	F	G	H
1		Expenses analysis using Ben			ford's Law			
2		Amount	First digit					
3		22500	2					
4		10750	1		First digit	Frequency	Frequency%	Bendford
5		8650	8		1	3	50.0%	30.1%
6		14200	1		2	1	16.7%	17.6%
7		16800	1		3	0	0.0%	12.5%
8		9500	9		4	0	0.0%	9.7%
9					5	0	0.0%	7.9%
10					6	0	0.0%	6.7%
11					7	0	0.0%	5.8%
12					8	1	16.7%	5.1%
13					9	1	16.7%	4.6%
14					TOTAL	6	100%	100.0%

By calculating the actual frequencies for the first leading digit of the above journal entries, we get:

(1) 50%

(2) 16.7%

(3) 0%

(4) 0%

(5) 0%

(6) 0%

(7) 0%

(8) 16.7%

(9) 16.7%

In this example, the actual frequencies for the leading digit do not match the expected frequencies according to Benford's Law, which could indicate that the expenses were manipulated or fraudulent. Further investigation would be necessary to determine the cause of the discrepancy and whether fraudulent activity occurred.

Illustration:

There were 500 cheque payment vouchers in a month. Out of this at least 150 (30% of 500) vouchers must begin with 1. It means cheques can be for Rs.19, Rs.100, Rs.100, 000 and so on.

The actual payments are stratified or segmented for transactions beginning with each digit and these transactions are counted and summarised as below.

First digit	*No of transactions*
1	165
2	88
3	63
4	49
5	38
6	33
7	28
8	26
9	10
TOTAL	500

As the head of forensic audit team, you are required to guide your team as to how they should proceed to unearth the fraud using Benford Law.

Solution:

First digit	*No of transactions*	*Frequency%*	*Benford*	*Variance*	*Remarks*
1	165	33.0%	30.1%	2.9%	Error/ Fraud expected
2	88	17.6%	17.6%	0.0%	
3	63	12.6%	12.5%	0.1%	
4	49	9.8%	9.7%	0.1%	
5	38	7.6%	7.9%	-0.3%	
6	33	6.6%	6.7%	-0.1%	
7	28	5.6%	5.8%	-0.2%	
8	26	5.2%	5.1%	0.1%	
9	10	2.0%	4.6%	-2.6%	Error/ Fraud expected
TOTAL	500	100%	100.0%		

The forensic team should focus on all the transactions having huge variances since Error or Fraud is expected applying Benford's law. This will help to detect whether fraud or error has happened in the entity.

Regression Analysis

Regression analysis is a statistical technique that examines the relationship between two or more variables. In fraud detection, regression analysis can be used to identify relationships between variables, such as the correlation between high-risk customers and suspicious transactions.

Suppose an insurance company wants to detect fraudulent claims made by its customers. The company collects data on the claims made by its customers, including the type of claim, amount of the claim, and other relevant details. The data is then analysed using regression analysis to identify relationships between the variables and detect any unusual patterns.

In this case, the company can use regression analysis to model the relationship between the amount of the claim and other relevant variables, such as the type of claim, the location of the claim, and the history of the claimant.

By using multiple regression analysis, the company can identify suspicious claims that are outside the normal behavior of its customers.

For example, if a regression model indicates that claims of a certain type and location are usually of a specific range of amounts, and a claimant suddenly files a claim outside that range, it may indicate fraudulent activity.

Additionally, the regression model can be used to compare the characteristics of these suspicious claims with past fraud cases to determine if they are similar or not.

Cluster Analysis

Cluster analysis is a statistical technique that groups similar data points together.

Suppose a credit card company wants to detect fraudulent activities in its transactions. The company collects data on the transactions made by its customers, including the transaction amount, location, time, and other

relevant details. The data is then analyzed using cluster analysis to identify patterns and groups of transactions that are similar to each other.

In this case, the company can use cluster analysis to group transactions based on their characteristics, such as the location, time, and amount of the transaction. The analysis can help identify clusters of transactions that are outside the normal behavior of the customers, and hence may be indicative of fraud.

For instance, if a cluster of transactions is identified that occurred at unusual locations and times, with higher than average transaction amounts, it may indicate fraudulent activity.

Additionally, the cluster analysis can be used to compare the characteristics of these suspicious clusters with past fraud cases to determine if they are similar or not.

Real life example

During Covid-19 lockdown time when no one was allowed to fly out of India, one of the customer of a credit card company got a confirmation call from the bank alerting in the middle of the night stating that his credit card has been swiped in Thailand. Whether the customer is approving it or not?

Having known that it was a fraudulent transaction purported to be attempt, the card was blocked at the request of the customer and the transaction was declined. This call was based on the automated suspicion report to protect the interest of its customers by the credit card company.

In fraud detection, cluster analysis can be used to identify groups of customers or transactions with similar characteristics, such as the same source of funds, similar transaction patterns, or unusual behavior.

Decision Trees

Decision trees are a machine learning technique used to classify data points based on a set of rules. In fraud detection, decision trees can be used to classify transactions or customers as high-risk or low-risk based on specific criteria.

Neural Networks

Neural networks are a machine learning technique used to identify patterns in data. In fraud detection, neural networks can be used to identify unusual transaction patterns or high-risk customers.

Anomaly Detection

Anomaly detection is a statistical technique used to identify unusual patterns in data. In fraud detection, anomaly detection can be used to identify unusual transaction patterns or customer behavior. “Too good to be true” gives a very good clue in anomaly detection.

Clustering Algorithms

Clustering algorithms are a machine learning technique that groups’ data points together based on similar characteristics. In fraud detection, clustering algorithms can be used to identify groups of high-risk customers or transactions based on specific criteria.

Gaussian Mixture Models (GMM), K-means clustering etc. can be used for fraud detection with the help of software tools.

Overall, statistical and mathematical techniques play a crucial role in fraud detection techniques, as they enable financial institutions to analyse large volumes of data and detect potential fraud patterns. These techniques, when used in combination with other fraud detection methods, can help to prevent and detect fraudulent activities.

TECHNOLOGY BASED FRAUD DETECTION TECHNIQUES

There are several technology-based fraud detection techniques that organizations can use to prevent and detect fraud.

Here are some of the most common techniques used across the world with the help of fraud detection software programs to detect irregular patterns. This is because of enormous volume of data flowing into the business it will be impossible to unearth the fraud by manually going through thousands of transactions due to time and manpower constraints.

Data Analytics

Data analytics involves using algorithms and statistical models to analyze large amounts of data and identify patterns, anomalies, and outliers that may indicate fraud. With the help of data analysis software it is possible to search entire data files for red flags of possible fraud. The number of checkpoints a forensic auditor or forensic accountant can set-up using a data analysis software is very high.

Data analysis can help the forensic auditor in developing reference files for fraud detection. He can establish a norm to enable him to compare individual months or years.

Machine learning

Machine learning (ML) is a subset of Artificial Intelligence (AI), is a learning algorithm in a computer system that enables it to identify patterns and outliers in a large data.

ML has the ability to uncover hidden patterns and allows the forensic auditor the ability to derive meaningful information from the big data.

Machine learning involves using algorithms to analyse historical data and learn from it, so that the system can automatically detect and prevent fraud in real-time.

Machine learning algorithms can analyse large datasets to detect patterns and anomalies that indicate fraudulent behavior. These algorithms can be trained using historical data to identify suspicious transactions and behaviors.

This approach is especially useful in detecting credit card fraud, insurance frauds, where transactions can be analysed in real-time to identify suspicious activities.

It is humanly impossible to detect credit card frauds, insurance frauds etc., manually because of huge volume of data. Hence, Machine learning is extensively used.

1. **Fraud Detection Machine Learning Algorithms Using Logistic Regression**:

   Logistic Regression is a supervised learning technique that is used when the decision is categorical. It means that the result will be either ‘fraud’ or ‘non-fraud’ if a transaction occurs.

   Case:

   Let us consider a scenario where a transaction occurs and we need to check whether it is a ‘fraudulent’ or ‘non-fraudulent’ transaction. There will be given set of parameters that are checked and, on the basis of the probability calculated, we will get the output as ‘fraud’ or ‘non-fraud.’ If probability calculated is 0.9, this means that there is a 90 percent chance that the transaction is ‘genuine’ and there is a 10 percent probability that it is a ‘fraud’ transaction.

2. **Fraud Detection Machine Learning Algorithms Using Decision Tree**:

   Decision Tree algorithms in fraud detection are used where there is a need for the **classification** of unusual

activities in a transaction from an authorized user. These algorithms consist of constraints that are trained on the dataset for classifying fraud transactions.

Case:

Let us consider a scenario where a user makes some transactions. Forensic auditor will build a decision tree to predict the probability of fraud based on the transaction made. First, in the decision tree, Machine will check whether the amount is greater than ₹50,000? If answer is 'yes,' then it will check the I.P address location from where the transaction is made. And if it is 'no,' then it will check the frequency of the transaction.

After that, as per the probabilities calculated for these conditions, it will predict the transaction as 'fraudulent' or 'non-fraudulent.'

For instance, if the amount is greater than ₹50,000 and location is equal to the IP address of the customer, then there is only a 25% chance of 'fraud' and a 75% chance of 'non-fraud.'

Similarly, if the amount is greater than ₹50,000 and the number of locations is greater than 1, then there is a 75% chance of 'fraud' and a 25% chance of 'non-fraud.'

Thus a decision tree in Machine Learning helps in creating fraud detection algorithms.

3. **Fraud Detection Machine Learning Algorithms Using Neural Networks**:

Neural Networks is a concept inspired by the working of a human brain. Neural networks in Deep Learning uses different layers for computation.

Neural networks uses cognitive computing that helps in building machines capable of using self-learning algorithms that involve the use of data mining, pattern recognition, and natural language processing. It is trained on a dataset passing it through different layers several times.

It gives more accurate results than other models as it uses cognitive computing and it learns from the patterns of authorized behavior and thus distinguishes between 'fraud' and 'genuine' transactions.

Artificial Intelligence

Artificial intelligence refers to computer systems that are able to mimic human-like tasks like visual perception and decision-making. Examples of artificial intelligence that we use every day without even realising it are: Auto Pilot function in flights, spam filters in email and mapping apps in smartphones to analyse the traffic congestion and suggest the fastest route.

Artificial intelligence (AI) involves using machine learning algorithms and other advanced technologies to analyse data, detect patterns, and identify potential fraud.

Biometric Authentication

Biometric authentication involves using unique physical characteristics such as fingerprints, iris scans, or facial recognition to verify the identity of individuals and prevent fraud. This technology is increasingly being used in various industries to prevent identity fraud.

Behavior Analysis

Behavior analysis involves monitoring user behavior to identify patterns of behavior that may indicate fraudulent activity. This can involve analysing user login patterns, transaction histories, and other behavioral data. Behavioral analytics involves the analysis of user behavior to detect patterns that may indicate fraudulent activities. This technique is commonly used in the banking and finance industry to detect account takeover fraud, where a fraudster takes over an account and performs unauthorised transactions.

Real-time Transaction Monitoring

Real-time transaction monitoring involves using automated systems to monitor transactions as they occur, and flagging suspicious activity in real-time.

Digital Signature Verification

Digital signature verification involves using technology to verify the authenticity of digital signatures on documents and transactions, to prevent fraud.

Data mining techniques

These are used to analyse large amounts of data to identify hidden patterns and co-relationships that may indicate fraudulent activities. This approach is commonly used in the insurance industry to detect fraudulent claims. This can include analysing transaction histories, user behavior, and other relevant data points.

Digital identity verification

Digital identity verification techniques are used to verify the identity of individuals who are accessing online services or making online transactions. This approach is commonly used in the e-commerce industry to prevent fraudulent activities. One time passwords are sent to the user to his or her mobile to change password or even to do online transactions.

Blockchain Technology

Blockchain technology can be used to create secure and transparent records of transactions, making it more difficult for fraudsters to alter or manipulate data.

Two-Factor Authentication

Two-factor authentication requires users to provide two different types of authentication, such as a password and a one-time code sent to their phone, to access an account. This can help prevent unauthorised access and identity theft.

These are just a few examples of the many technology-based fraud detection techniques that organizations can use to prevent and detect fraud.

By leveraging advanced tools and techniques, businesses can better protect themselves and their customers from fraudulent activities.

DIGITAL FORENSICS TECHNIQUES

Digital forensics is the process of collecting, preserving, analyzing, and presenting electronic data in a way that is admissible as evidence in a court of law. This includes retrieving data from computers, mobile devices, and other digital storage media to support legal cases.

Digital Evidence

In order to solve a cybercrime alleged to have been committed appropriate digital evidence have to be identified and collected, analysed and evaluated as to the suitability in the court of law and report have to be prepared by the digital forensic expert and submitted to those who have appointed him.

Fraud investigation will involve searching for and potential recovery of digital documents such as invoices, statements, order forms, spreadsheets and databases. Emails can also be a good source of information relating to fraud. It can contain information concerning contact between fraudsters, the passing of information such as credit card and bank account details.

The initial stage of dealing with the digital forensics aspect of a fraud detection investigation is capturing the data. Whether this is done by the police or by a forensic auditor on their behalf, the procedures are the same.

Information and evidence can be obtained from servers, workstations, laptops, removable storage media, mobile phones and other handheld devices of the entity. The collection of the data should be carried out by a trained and experienced person, in a manner which does not allow the original data to be altered in any way.

The process of capturing the data in such a secure manner is known as 'acquisition' or 'imaging'. It is achieved by capturing through a write protection device a very low level copy of the contents of the media. This, once processed, allows the investigator a view of the contents of the computer including those areas that would not normally be visible to a user. This is known as a forensic image.

The two tools most widely used for the processing and examination of a forensic image are 'EnCase' (produced by Guidance Software) and 'Forensic ToolKit' or 'FTK' (produced by AccessData). These allow the investigator to view the content of the images, conduct searches and potentially retrieve hidden and deleted data.

There are tools available which will attempt to recover items such as social networking chat logs and other artefacts, which may be missed. These items can be very helpful in a fraud detection investigation, as often, communication happens between culprits through instant messaging or 'Chat' on websites such as 'Facebook'.

Additionally, a record of Internet history can provide information that would be very useful to an investigator. For example, the fact that the Internet history on a suspect computer has entries of having visited various online banking websites, could indicate that a user with fraudulent intent has been visiting accounts of their targets. Mobile Forensics and Botnet Forensics are other important fraud detection techniques.

Digital forensics has been discussed at length in Chapter 14 Cyber Forensics

DATA MINING TECHNIQUES FOR FRAUD DETECTION

Data mining techniques have become increasingly important in fraud detection due to the sheer volume of data that needs to be processed and analysed in order to identify potentially fraudulent behavior. Employees using company credit cards for personal expenses, employees claiming reimbursement of expenses on a day they were not travelling are some examples.

Some common data mining techniques used in fraud detection are:

1. **Anomaly Detection:**

   This technique involves identifying data points that deviate significantly from the norm or expected patterns. This is called as outliers. In fraud detection, it can be used to identify transactions or behaviors that are unusual and may be indicative of fraud.

   For example regularly logging outside office hours and on holiday, or from a remote IP address are all anomalies which are used during investigation to detect manipulation of financial records and transactions fraudulently.

2. **Clustering:**

   This technique involves grouping similar data points together. In fraud detection, clustering can be used to group similar transactions or behaviors together, making it easier to identify patterns of fraudulent activity.

3. **Decision Trees:**

   Decision trees are graphical representations of decisions and their possible consequences. In fraud detection, decision trees can be used to create rules that identify potentially fraudulent behavior based on a series of criteria.

4. Neural Networks:

Neural networks are a type of machine learning algorithm that can learn from data and identify patterns. In fraud detection, neural networks can be used to identify complex patterns of fraudulent behavior that may not be immediately apparent.

5. Text Mining:

Text mining involves analysing unstructured text data, such as emails or chat logs. It is a method of using a specialised software to extract information from unstructured text data.

Through the application of linguistic technologies and statistical techniques, fraud keywords that are likely to point suspicious activity are mined from the texts.

Example of fraud keywords can be deadline, trouble, quota, short, concern, problem, override, write-off, adjust, reserve/provision, reasonable, deserve, temporary etc., are mined from the text by analysing the digital written communication or in the journal entries.

This list depend on the nature of industry, fraud scheme and the data set the forensic auditor. It also depends on whether they are searching emails or accounting records.

In the case of suspected bribery or corruption words in payment description can include consulting fees, goodwill payment, processing fee, donation, special commission, special payment, expediting fee, one-time payment and so forth.

In the text mining the emotional tone of the correspondence in emails and other digital messages, derogatory, surprised, secretive, worried and angry emotions communications can be used for detecting frauds.

In fraud detection, text mining can be used to identify suspicious language or topics that may be indicative of fraud.

6. Association Rules or Link Analysis:

Association rules are used to identify relationships between different variables. In fraud detection, association rules can be used to identify patterns of behavior that are commonly associated with fraudulent activity.

Data mining techniques can be very useful in identifying patterns of fraudulent behavior and detecting potential fraud. However, it is important to use these techniques in conjunction with other fraud detection methods, such as manual review and investigation, in order to ensure that accurate and actionable results are obtained.

WILFUL DEFAULTS AND EMERGING FORENSIC AUDIT ASPECTS UNDER INSOLVENCY AND BANKRUPTCY CODE, 2016

The term “wilful default” refers to a deliberate and intentional act of non-repayment of a loan or debt by a borrower despite having the ability and means to repay. It is a deliberate act of avoiding the payment. It is considered a serious offence under the Insolvency and Bankruptcy Code, 2016 (“IBC”). This is because it can result in significant financial losses for the lender and seriously impacts the financial system.

Under the IBC, a creditor can initiate insolvency proceedings against a borrower who has committed a wilful default. The creditor must first provide evidence to the insolvency resolution professional that the borrower has committed a wilful default. The insolvency resolution professional will then examine the evidence and determine whether the borrower has indeed committed a wilful default.

If the insolvency resolution professional finds that the borrower has committed a wilful default, the borrower may be barred from participating in the insolvency resolution process. The insolvency resolution professional may also recommend criminal proceedings against the borrower and its management for fraud or other offences.

"Wilful default" means "conscious and deliberate non-payment of dues by the corporate debtor despite having adequate means to pay, or the diversion of funds for purposes other than for which the loan was availed, or siphoning off funds so that it appears that the corporate debtor has become financially incapable of repaying the loan."

It is important to note that the determination of whether a borrower has committed a wilful -default is a fact-specific inquiry, and each case will depend on the particular circumstances involved. Factors that may be considered in making this determination include the borrower's financial condition, the borrower's ability to repay the loan, and the borrower's conduct in relation to the loan.

Under the Insolvency and Bankruptcy Code (IBC), wilful default is a serious offense, and the IBC provides for stringent penalties for defaulting borrowers who have acted willfully.

If a borrower is found to have acted willfully, the IBC empowers the creditor to initiate insolvency proceedings against the borrower. The wilful defaulter is not eligible for any concessions or exemptions, and the resolution process would be conducted without any moratorium or stay on legal proceedings. The wilful defaulter may also face criminal proceedings, which could result in imprisonment, fines, or both.

Emerging Forensic Audit Aspects under Insolvency and Bankruptcy Code, 2016

Forensic audit plays a crucial role in detecting and investigating frauds, irregularities, and non-compliances in insolvency and bankruptcy cases under the Insolvency and Bankruptcy Code, 2016 (IBC).

IBC is still a relatively new law, there are several emerging forensic audit aspects that are gaining importance in resolving insolvency and bankruptcy cases.

Some of these aspects are:

Pre-insolvency Forensic Audit:

Conducting a pre-insolvency forensic audit of the debtor's financial statements and records can help identify potential frauds, non-compliances, and irregularities that could impact the insolvency resolution process. This can help the resolution professional (RP) and the committee of creditors (CoC) in making informed decisions during the resolution process.

Investigation of Preferential Transactions:

Forensic audit can help investigate preferential transactions, which are transactions made by the debtor with related parties or other creditors to give them an unfair advantage over other creditors. Forensic audit can help identify such transactions and recommend actions to be taken to recover the assets involved.

Identification of Undisclosed Assets:

Forensic audit can help identify undisclosed assets of the debtor, which could be used to repay the creditors. This could include assets that were intentionally hidden by the debtor or those that were not disclosed due to negligence or oversight.

PUFE transactions by a debtor before the initiation of insolvency proceedings:

PUFE transactions refer to Preferential, Undervalued, Fraudulent, and/or Extortionate transactions that are made by a debtor before the initiation of insolvency proceedings under the Insolvency and Bankruptcy Code, 2016 (IBC) in India.

These transactions can significantly impact the insolvency resolution process, as they can reduce the assets available to repay the creditors.

Under the IBC, the resolution professional (RP) is required to examine all transactions made by the debtor during the relevant period to identify PUFE transactions. The relevant look back period is the period of two years preceding the insolvency commencement date.

If the RP identifies any PUFE transactions, they are required to make an application to the National Company Law Tribunal (NCLT) to declare such transactions as void. Once a transaction is declared void, the property or asset involved in the transaction is deemed to be vested with the debtor and becomes a part of the assets of the debtor's estate.

The IBC defines various types of PUFE transactions, as follows:

Preferential transactions: Section 43 of IBC

These are transactions made by the debtor to prefer one creditor over others. These transactions can be avoided if they were made within two years preceding the insolvency commencement date and the creditor had reasonable knowledge of the debtor's financial position.

IDBI Bank Ltd. v. *Jaypee Infratech Ltd.* **(***JIL***)** is a perfect example of transaction to be considered as preferential transaction.

The Allahabad Bench of the National Company Law Tribunal ("NCLT") observed that, the timing of entry of the transaction by JIL was questionable and JIL had entered into this transaction when it was facing severe financial difficulty". The Tribunal further observed that, the impugned transactions were entered into within the relevant period and are preferential transactions under Section 43 of the Code.

Undervalued transactions: Section 45 of IBC

These are transactions made by the debtor at a significantly lower value than the fair market value of the property or asset involved. These transactions can be avoided if they were made within two years preceding the insolvency commencement date.

Fraudulent transactions: Section 66 of IBC

These are transactions made by the debtor with an intention to defraud the creditors or any other person. These transactions can be avoided if they were made within two years preceding the insolvency commencement date.

The Supreme Court in (*M/s Embassy Property Developments* v. *State of Karnataka & Others*) laid down that NCLT and NCLAT have the jurisdiction to inquire into fraudulent transactions under section 66.

Extortionate transactions: Section 50 of IBC

These are transactions made by the debtor at an excessive price or amount in comparison to the prevailing market rates. These transactions can be avoided if they were made within two years preceding the insolvency commencement date.

Detection of Fraudulent Transactions:

Forensic audit is involved when there several entities / huge transactions involved, showing assets stripping/ funds diversions / Round tripping and fraud observed; Forensic Audit – runs beyond 2 years.

Forensic audit can help detect fraudulent transactions made by the debtor, including those made to siphon off funds, inflate revenues or assets, or misrepresent financial statements. Such transactions can be investigated and reported to the Committee of Creditors and the National Company Law Tribunal (NCLT).

Investigation of potential wrongdoing by promoters:

Forensic audit can also help investigate potential wrongdoing by the promoters of the debtor company, including mismanagement, diversion of funds, and other fraudulent activities that could have led to the insolvency or bankruptcy of the company.

CASE LAWS

Case laws on IBC, 2016

National Company Law Appellate Tribunal - *M. Srinivas vs. Ramanathan Bhuvaneshwari*

Resolution Professional filed application under section 66 of IBC for recovery of Rs. 46 crore, being receivables, inventory and P & M diverted; Adjudicating Authority ordered directed Central Government to initiate investigation by SERIOUS FRAUD INVESTIGATION OFFICE (SFIO) ; Now Ministry of Corporate Affairs investigation is on, based on National Company Law Appellate Tribunal (NCLAT) orders, modifying order of Adjudicating Authority.

National Company Law Tribunal (Mumbai) - *Rama Ratan Kanoongo vs. Sunil Kathuria*

Resolution Professional (RP) filed application for Liquidation of Corporate Debtor (CD); RP also sought for recovery of Rs.135 Lakhs being preferential transaction with one of the respondents;

NCLT Mumbai observed that this transaction was not done in the ordinary course of business of CD, as stock has been transferred and no payment has been made for the same; The transaction is satisfying the criteria of Section 43 of the Code and is to be labelled as preferential transaction and the prayers of the Applicant are allowed.

Adjudicating Authority also ruled that the treatment of avoidance or preferential or undervalued transaction is applicable even at the stage of liquidation.

LESSON ROUND-UP

- **Fraud:** Wrongful or criminal deception intended to result in financial or personal gain.
- **Investigation:** The action of investigating something or someone; formal or systematic examination or research.
- **Detection:** The action or process of identifying the presence of something concealed.
- **Fraud detection** is the process of identifying and preventing fraudulent activity in various contexts, including financial transactions, online interactions, insurance claims, and more. It is an important tool for individuals and organizations to protect themselves against financial losses and reputational damage caused by fraud. It is a postmortem after the alleged fraud has happened and a reactive action.
- **Early warning indicators of Fraud** such as Unusual Financial Activity, Poor Accounting, Unusual behavior, Unexplained Inventory, Employee Turnover, Weak or lack of Internal Controls, Complaints or Tip, Weaknesses in IT Security, Suspicious Emails or Messages
- **Money laundering** starts with proceeds from a specific source. For a variety of reasons the launderer wants to hide the money trail. Money laundering takes place in three distinct stages: Placement, Layering and Integration. The money launderers including drug dealers, fraudsters, tax evaders and terrorists have many challenges when moving money through each of the stage.

- The responsibilities of the external auditor as they relate to fraud detection are clearly defined in International Standard on Auditing (ISA-240), The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements.

  "The auditor is responsible for maintaining professional skepticism throughout the audit, considering the potential for management override of controls, and recognizing the fact that audit procedures that are effective for detecting error may not be effective in detecting fraud. The requirements in this are designed to assist the auditor in identifying and assessing the risks of material misstatement due to fraud and in designing procedures to detect such misstatement"

- **Statistical and mathematical techniques** play a crucial role in fraud detection techniques, as they enable financial institutions to identify and analyze large volumes of data to detect potential fraud patterns.
- **Benford's Law** is a statistical tool used to detect potential fraud in financial statements or other numerical datasets. The law states that in many naturally occurring datasets, the leading digit is more likely to be a small number (e.g., 1, 2, or 3) than a large number (e.g., 8 or 9). One application of Benford's Law is in detecting fraudulent journal entries or fraudulent financial transactions in the books of account.
- **Regression Analysis** is a statistical technique that examines the relationship between two or more variables. In fraud detection, regression analysis can be used to identify relationships between variables, such as the correlation between high-risk customers and suspicious transactions.
- **Cluster Analysis:** Cluster analysis is a statistical technique that groups similar data points together.
- The term **"wilful default"** refers to a deliberate and intentional act of non-repayment of a loan or debt by a borrower despite having the ability and means to repay. It is a deliberate act of avoiding the payment. It is considered a serious offence under the Insolvency and Bankruptcy Code, 2016 ("IBC"). This is because it can result in significant financial losses for the lender and seriously impacts the financial system.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

Multiple Choice Questions (MCQs)

1. Act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity is called

   A. email bombing

   B. Spamming

   C. Cyber stalking

   D. Phishing

2. An activity that uses accounting, auditing and investigative skills to assist in legal matters, is known as:
    A. Fraud Audit
    B. System Audit
    C. Forensic Audit
    D. Due Diligence
3. 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, is known as:
    A. Forensic Accounting
    B. Forensic Audit
    C. Forensic Investigation
    D. None of the above
4. Know your Customer (KYC) regulations have been introduced in financial transactions under which of the following Act?
    A. Prevention of Money Laundering Act
    B. Companies Act
    C. Reserve Bank of India Act
    D. Banking Regulations Act
5. Which are the following steps in Money Laundering: Placement, Layering, Integration and Counterfeiting
    A. Only 2 and 4
    B. 1, 2 and 4
    C. 1, 2 and 3
    D. 1, 2, 3 and 4

Answer: (1) D (2) C (3) A (4) A (5) C

Practice Questions

1. What are the early warning indicators of fraud to be kept in mind by a forensic auditor?
2. Explain some of the common techniques used for fraud detection in money laundering.
3. Explain how Benford's law can be used a tool in fraud detection technique.
4. Explain the Data Mining techniques adopted by forensic auditors in Fraud Detection.
5. Explain the Statistical and Mathematical Techniques adopted by forensic auditors in Fraud Detection.
6. Discuss in detail emerging forensic audit aspects under Insolvency and Bankruptcy Code, 2016.
7. Explain the terms PUFE under the IBC, 2016 with examples.

LIST OF FURTHER READINGS

- **Forensic Audit Decoded**

  Author: G.C. Pipara

  Publishers: Taxmann

- **Forensic Audit**

  Author: CA Kamal Garg

  Publishers: Bharat's

WARNING

Regulation 27 of the Company Secretaries Regulations, 1982

In the event of any misconduct by a registered student or a candidate enrolled for any examination conducted by the Institute, the Council or any Committee formed by the Council in this regard, may suo-moto or on receipt of a complaint, if it is satisfied that, the misconduct is proved after such investigation as it may deem necessary and after giving such student or candidate an opportunity of being heard, suspend or debar him from appearing in any one or more examinations, cancel his examination result, or registration as a student, or debar him from re-registration as a student, or take such action as may be deemed fit.

It may be noted that according to regulation 2(ia) of the Company Secretaries Regulations, 1982, 'misconduct' in relation to a registered student or a candidate enrolled for any examination conducted by the Institute means behaviour in disorderly manner in relation to the Institute or in or around an examination centre or premises, or breach of any provision of the Act, rule, regulation, notification, condition, guideline, direction, advisory, circular of the Institute, or adoption of malpractices with regard to postal or oral tuition or resorting to or attempting to resort to unfair means in connection with writing of any examination conducted by the Institute, or tampering with the Institute's record or database, writing or sharing information about the Institute on public forums, social networking or any print or electronic media which is defamatory or any other act which may harm, damage, hamper or challenge the secrecy, decorum or sanctity of examination or training or any policy of the Institute.

PROFESSIONAL PROGRAMME
INTERNAL & FORENSIC AUDIT
GROUP 1 • ELECTIVE PAPER 4.2

(*This test paper is for practice and self-study only and not to be sent to the Institute*)

Time allowed: 3 hours *Maximum Mark: 100*

Answer all Questions

PART I - INTERNAL AUDIT (60 MARKS)

Question No. 1

(a) ABC Ltd. (major player in automobile industry) appoints M/s Sahni and Co. to conduct an Internal Audit. Mr. A, an article assistant in M/s Sahni and Co., while conducting an internal audit undertake informal oral inquiries with staff of ABC Ltd. During this process, one of the staff member of ABC Ltd. revels to Mr. A about a cash related fraud committed by cashier. In order to go deep to reveals about the fraud, Mr. A had a discussion with senior officer in Accounts department and concluded that cash related fraud has been committed by cashier. Mr. A asked for the written confirmation from the staff and officers in the accounts department but both had refused to give any written confirmation and denied that fraud have been committed.

What will be the next course of action by Mr. A as an Internal Auditor?

(8 Marks)

(b) Aruna Ltd, a listed company, headquartered in Mumbai, Maharashtra has appointed M/s Rao and Co (Practicing Company Secretaries) to conduct an internal audit of the company. The internal auditor, during the review of tax liabilities of GST with respect to goods and services provided during the period under audit, reveals that a total of around 1000 transactions (valued around Rs. 1500 crore) goods and services have been provided wherein incorrect GST rates were applied (9% has been charged instead of 18%) resulting into excess GST liability.

In this situation, what should be the next course of action of the Internal Auditor?

(7 Marks)

Question 2

(a) Moon Limited, a listed company, headquartered in Delhi, is in the business of providing hi-tech consulting services in India as well as globally. It has around 135 client base in India and around 45 clients outside India to whom it provides hi-tech consulting services inclusion technology based solution.

Moon ltd. has around 1000 employees and having in house Internal Audit Department. Further, it appoints Mr. Sujan and Co. (Practicing Company Secretary) for conducting internal audit. During the period under review, the internal auditor (Mr. Sujan) observed that there are few employees to whom appointment letter has not been issued and further there are no mechanism to capture in and out time of those employees.

This matter has been brought to the notice of the management by the internal auditor. Management stated that these employees are trainee for 2-3 months and therefore appointment letter has not been

issued to them. Further, very small amount is paid as stipend and therefore, in-time and out-time of the trainees are not captured.

In this situation, what should be the next course of action of the Internal Auditor?

(8 Marks)

(b) While conducting the Internal Audit of the Company, the internal auditor has observed the following while reviewing the employees official travelling expenses:

(i) Not able to trace the request and approval for travelling. Also, the travelling record does not reveals the reason of travel.

(ii) Employees mostly travelled by their own vehicle and claimed reimbursement on the basis of kilometer travelled. No other supporting documents were attached to substantiate the travel actually performed.

(iii) In case of travels performed by Air where boarding passes were missing as a proof of travel.

In this situation, what action should be taken by the Internal Auditor?

(7 Marks)

Questions 3

(a) A firm comprising of two partners who take active part in running the vegetable business, with two assistants. The firm has simple accounting system and does not need more than a cash and bank book to record. Expenses such as rent and insurance, Purchase of vegetables like cabbages, carrot, potatoes, onion etc. Sale of vegetables etc.

The expenses and purchases are supported by two box files of “paid” and “unpaid invoices” and they have billing machine to record sales.

As an internal auditor how would you ensure that sales and purchases were completely and accurately recorded?

(b) The office manager controlled the company’s financial operations. She did payroll, accounts payable, invoicing and cash receipts. She rarely took time off, and even then, came back when they needed to run checks or payroll. The owner viewed her as key to running the business. What are your recommendations as an internal auditor of the organizations in view of evaluating Internal Control Mechanism?

(c) ABC Pvt. Ltd. having Rs. 90 lacs paid-up capital, Rs. 5 crores reserves and turnover of last three consecutive financial years, immediately preceding the financial year under audit, being Rs. 50 crores, Rs. 175 crores and Rs. 300 crores, but does not have any internal audit system. In view of the management, the internal audit system is not mandatory. Comment?

(5 Marks Each)

(Attempt Either Q. No. 4 OR 4A)

Questions 4

(a) Mr. ABC is the chief Internal Auditor of M/s XYZ Pharmaceuticals Private Limited. The company has spread its sales operations across 20 countries through Distributors and Dealers network. For the purpose of local connections and compliances, the Company has opened branch offices in each country. Apart from this, the Company has manufacturing facilities in India and China. For the purpose

of manufacturing raw material, technology is imported from various countries including USA, France and Japan. The key statistics of the company are mentioned below:

1. Annual Turnover of the Company – Rs. 25,000 crores approx.
2. Total Manpower – 8000 employees
3. Total Branches – 18

Audit Committee has asked Chief Internal Auditor (CIA) to prepare audit plan for 3 years. Please suggest the steps to be followed by the CIA and prepare audit universe of the Company.

(b) XYZ advisors is a management consulting firm having 250 fortune company client base. The CEO of the company is concerned about high employee attrition rate in his company. He has given assignment to dig out the reason for such high attrition rate as well as way forward. What factors would an Internal Auditor consider while conducting such analysis?

(c) Briefly narrate the difference between Internal and Statutory Auditor?

(5 Marks Each)

Question 4A

I. Internal auditor carried out a physical verification of Fixed Deposit Receipts on a surprise basis and tallied it with the Ledger balance. Finding no discrepancy the auditor submitted an assurance report. Finance head expressed the view that since this exercise was always carried out by the statutory auditors at the end of the year, this was a redundant exercise.

What should be the response of Internal Auditor in this situation?

II. State with reasons (in short) whether the following statements are correct or incorrect:

(i) "Audit Documentation", the working papers are not the property of the auditor.

(ii) Purchase invoice is an example of internal evidence.

(iii) Sufficiency is the measure of the quality of audit evidence.

(iv) Inquiry alone is sufficient to test the operating effectiveness of controls.

(v) Universe refers to the entire set of data from which a sample is selected and about which the auditor wishes to draw conclusions.

III. The paid-up share capital X Private Ltd. as on 31.03.2023 is Rs. 1.50 crores. The reserves and surplus as on that date is Rs. 30 lakhs. The turnover of X Private Ltd as per Profit and loss account for financial years 2019-20, 2020-21 and 2021-22 are as follows:

Financial Year	Turnover (Rs. in crores)
2019-20	7
2020-21	12
2021-22	15

Will the company be exempt from CARO, 2020 for the financial year 2022-23?

(5 Marks Each)

PART II – FORENSIC AUDIT (40 MARKS)

Question 5

Shree Capital, a 'NBFC', registered and having banking license to operate, perform and channelize the banking operation in the district of Kolhapur (Maharashtra). The banks headquarter is situated at Kolhapur and having 12 branches situated at various remote locations in the district of Kolhapur.

Objectives: The main objects of the Shree Capital is to provide crop agriculture loans (grapes loan) to the farmers (who involved in producing the grapes) in remote location in the district of Kolhapur. The loan granted to the farmers were without any collateral security and therefore categorized as personal loan.

Financial Performance: The Financial Statement of the Shree Capital showing the net profit (increasing trends) for last 4-5 years and reflecting Non-Performing Assets 'NPA' less than 0.5% in previous years .

On the other hand, the farmer's wealth conditions in the district of Kolhapur got worse during the last 4-5 years, due to crop destroyed on account of bad weather conditions.

Preliminary Investigation: Based on preliminary investigation, the following facts are revealed:

(i) The Kolhapur districts have two sugar factories. The local farmers also worked (part time) in these factories to earn their livelihood.

(ii) The financial condition of sugar factories are not good for last 4-5 years and the local banks have refused to provide loan assistance to the sugar factories.

(iii) Despite of financial crisis, the sugar factories smoothly carried out the production process.

(iv) Banks senior employees have good connect with the management team of the sugar factories.

(v) In the books of account of the banks, all the 12 EMI's for the year (with respect to loan granted to farmers) were collected on the last day of the previous year and not on monthly basis.

(vi) The personal wealth of the senior employees of the bank was increased 4 times in past 4-5 years.

(vii) The bank's documentation regarding the loan requisition form, sign etc. were properly maintained.

On the basis of the above, draw up a plan of action which you will adopt to fulfill your work to (suitable assumption may be made by you) indicate your approach in the following areas:

(a) Detailed Methodology.

(b) Findings of the case based on your methodology.

(c) Limitations of the forensic report.

(d) Legal steps that could be taken against NBFC, its subsidiaries and their directors.

(5 Marks each)

(Attempt Either Q. No. 6 OR 6A)

Question 6

(a) Mr. X received an email from the Income Tax Dept., mentioning the following :

> Dear Taxpayer,
>
> You have filed your income tax return for the Assessment Year 2023-24 and a refund of Rs. 14,600 is payable to you. However, the account mentioned by you is incorrect and requires validation.

> Please visit the following link in order to validate your account.
>
> *http:/jncometaxindiafiling.jov.com*
>
> *Note:* Failure to validate your account number will lead to rejection of refund.
>
> Regards Team : Income Tax Department
>
> Pay tax honestly and contribute in Nation's Development

What Mr. X should do in the mentioned situation?

(10 Marks)

(b) Arjun Ltd. is a registered supplier of spare parts of spinning mills and covered under the GST law. Their turnover for the year ended 31st March, 2022 is Rs. 800 crores and they have filed their return of income on 6th September, 2022.

Arjun Ltd. borrowed a working capital (cash credit limit) from a bank of Rs. 150 Crore. Arjun Ltd. regularly submit the month end closing stock statements of each month to bank without delay.

A bank suspects that the stock statements furnished by Arjun Ltd for the last 12 months do not reflect the true position and that they have been systematically furnishing statements showing higher quantities of various items of stock as compared to the actual quantity present in their godowns, and also that the values have been overstated.

The bank has appointed you as the forensic auditor. Explain, how will you go about gathering evidence and what are the documents, statements, returns, etc., you will go through to check the veracity of the stock statements furnished by the borrower?

(10 Marks)

Question 6A

(i) What is 'Red Flag' and 'Green Flag'? What are the indicators of 'Red and Green Flag'? Illustrate with examples.

(ii) Explain with example "Fraud Triangle".

(iii) What is Fraud?

(vi) Explain with examples 5 types of Cyber Crime?

(5 Marks each)