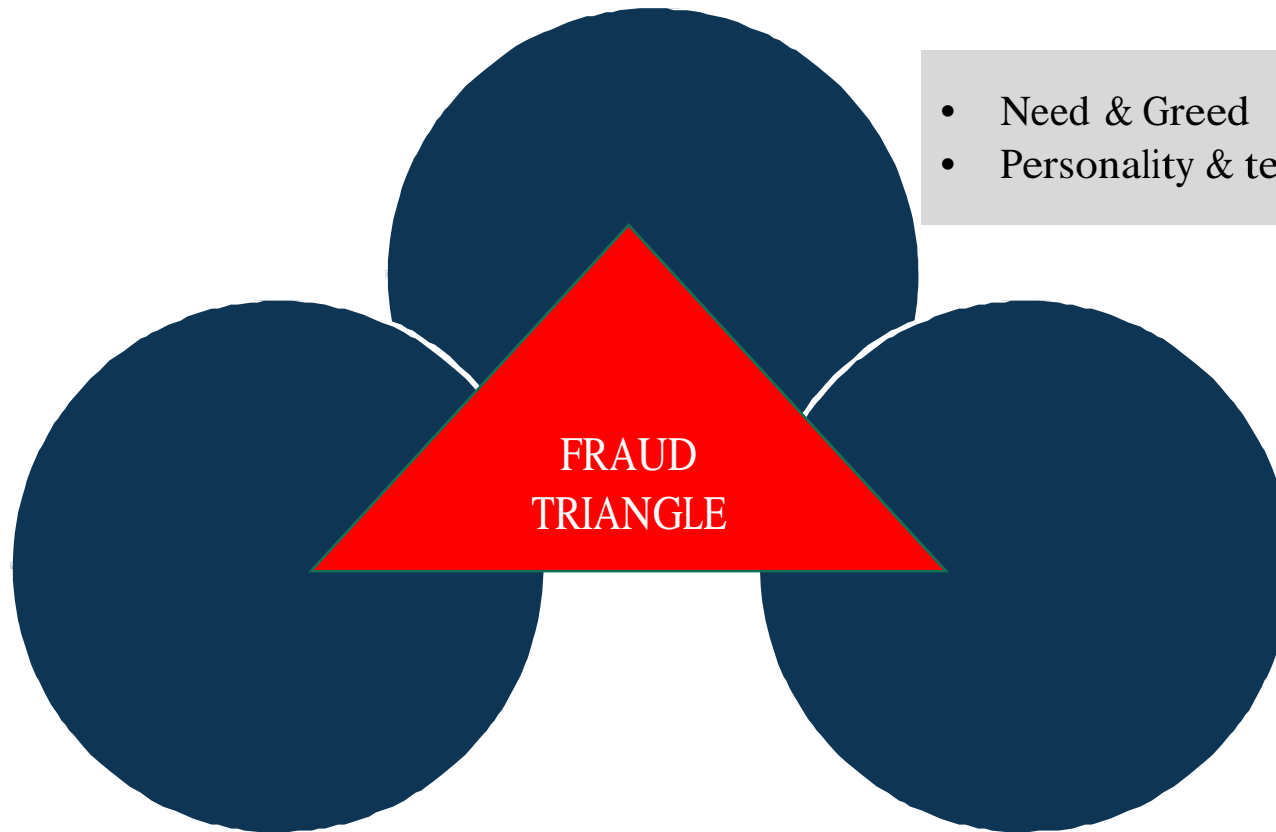




Fraud Investigation methodologies and Report Structuring

CA Pradeep Godbole

Why do people commit fraud – Fraud Triangle



- Need & Greed
- Personality & temperament

- Weak internal control system
- Poor security over assets
- Lack of fear of detection
- Unclear policies

- Fear of getting shamed / caught
- Necessary
- Harmless
- Justified

Legal & Regulatory Framework



- Indian Penal Code (IPC)
- Code of Criminal Procedures 1973
- Indian Evidence Act 1872
- Indian Contract Act 1872
- Companies act, 2013
- Regulatory requirements like RBI for banking
- Information Technology Act 2000
- Prevention of Corruption Act
- Prevention of Money Laundering Act

Types of Frauds

Cross Industry

- Asset misappropriation and theft
- Fraudulent handling of cash receipts
- Fraudulent disbursements
- Bribery and corruption
- Theft of intellectual property
- Consumer fraud
- Employee fraud
- Vendor / contract / procurement fraud

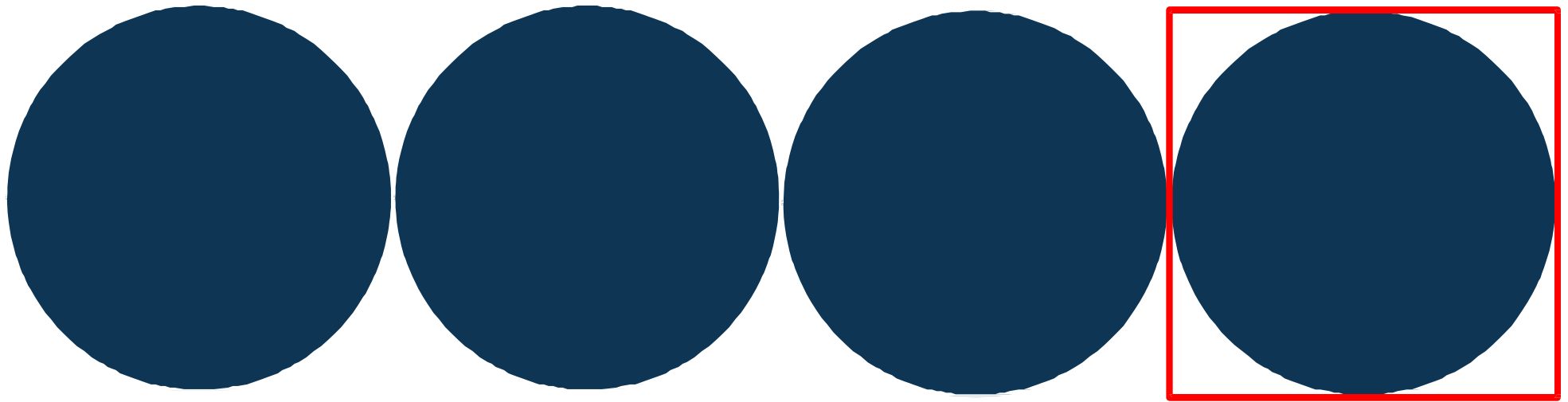
Industry specific

- Credit fraud
- Check and credit card fraud
- Insurance fraud
- Healthcare fraud
- Securities fraud
- Investment scams
- Bankruptcy fraud

Regulatory Driven

- Fraudulent financial statements
- Money laundering
- Tax fraud
- Cyber fraud

Components of Fraud Management



Objectives of Fraud Investigation

- Identifying improper conduct
- Identifying the persons responsible for improper conduct
- Determining the extent of potential liabilities or losses that might exist
- Preventing fraud and possible future frauds / losses
- Helping to facilitate the recovery of losses
- Mitigating other potential consequences
- Strengthening internal control weaknesses
- Sending a message throughout the organization that fraud will not be tolerated
- Regulatory / legal requirements

Investigation should be undertaken in the event that a fraud incident occurs, or suspicion of a fraud arises.

Principles of fraud investigation

- Assume litigation will follow – gather evidence in proper manner
- Act on predication - Predication is the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe that a fraud has occurred, is occurring, and/or will occur
- Approach with two perspectives – a) fraud has occurred or b) fraud has not occurred
- Move from general to specifics
- Confidentiality
 - Avoid alerting the suspected fraudster(s)
 - Request participants' confidentiality
 - Guard case information

Fraud Response Plan

- Fraud response plan
 - Reporting protocols
 - Response team responsible for conducting an initial assessment
 - Factors used to decide on the course of action
 - Litigation hold procedures
 - Principles for documenting the response plan
 - Template or form to report fraud incidents

Fraud Investigation Process

- Activate response team
- Internal - external communication
- Immediate actions
- Initial assessment plan

- Initial analysis
- Interview source
- Interview key individuals
- Evidence gathering
- Documentation
- Initial predication

- Fraud Theory Approach

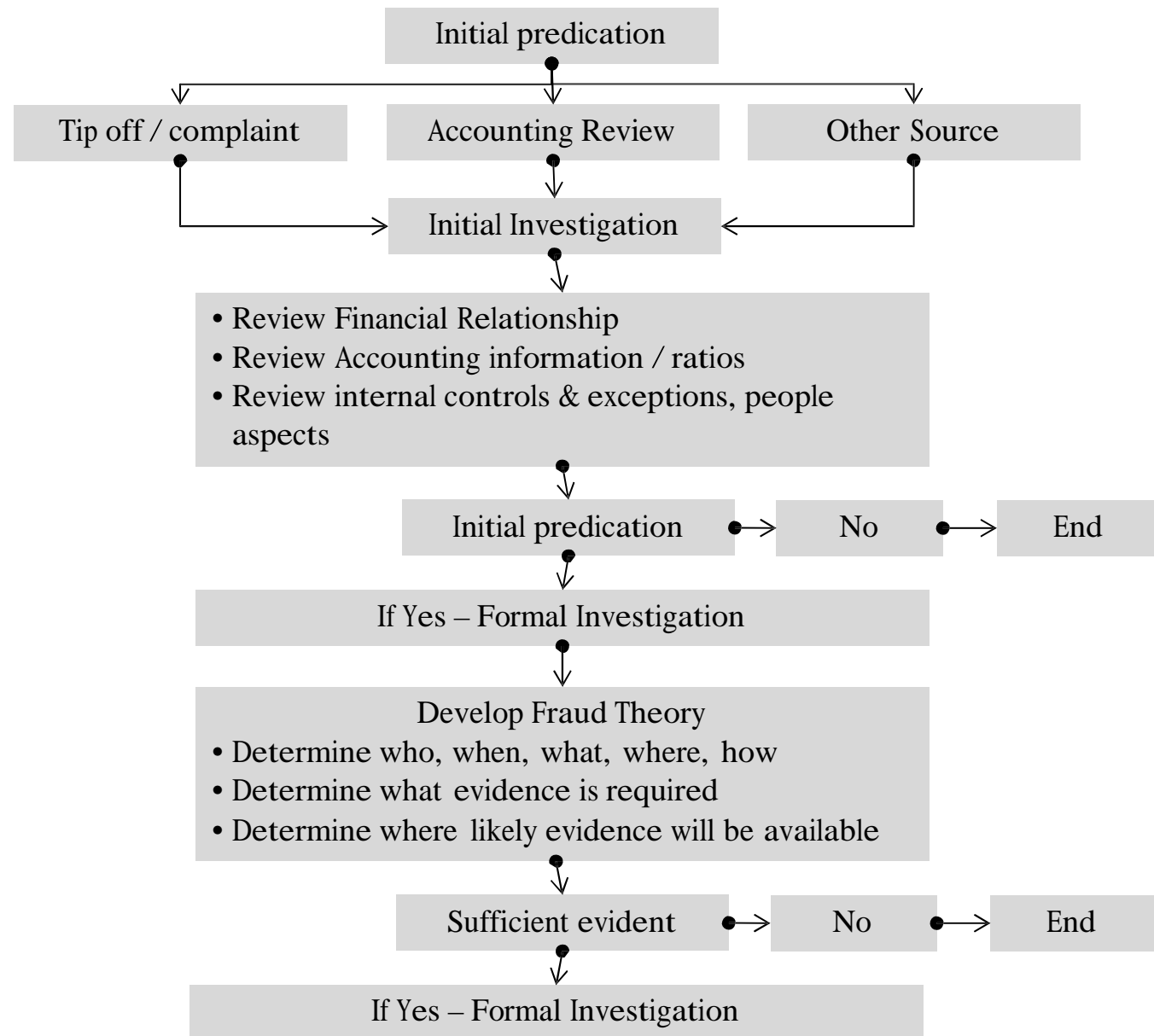
- Form Fraud Investigation Team
- Fraud Investigation Plan

- Use appropriate fraud investigation techniques
- Gather evidence
- Documentation

- Draw conclusions based on evidence gathered
- Reporting

Fraud Theory Approach

- Fraud theory approach
 - Analyzing available data
 - Creating a hypothesis
 - Testing the hypothesis
 - Refining and amending the hypothesis



Fraud Investigation Techniques

[Redacted]		
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

Every fraud incident is different and the response and investigation methods will vary depending on the facts that are unique to each case

Investigative intelligence and analysis

- Research on publicly sourced information, obtaining relevant information concerning individuals and entities suspected of involvement in the fraud. Typical sources of information
 - Social media
 - News items in the media
 - Registrar of companies or for directorships and shareholdings
 - Court judgements

Document Analysis

- Analyzing documents
 - Obtain documentary evidence – direct / circumstantial
 - Fraudulent documents
 - Organization of evidence

Forensic Accounting and Transaction Analysis

- Forensic accounting is the use of professional accounting skills in matters involving potential or actual civil or criminal litigation. The focus is on exceptions, irregularities and patterns of conduct
- Forensic accountants a) proactively investigate the control environment to identify weaknesses and areas susceptible to fraud or loss or b) investigate a specific situation to ascertain the true financial position where transaction may have happened but the cause is unknown or transaction is deliberately recorded to misstate financial statements
- Possible areas of material misstatement – a) revenue recognition b) expense understatement c) asset overstatement d) understatement of liabilities e) inventory variance f) improper disclosure
- Forensic accounting process involves
 - Walk through of business cycle and observing controls
 - Focus on red flags and cultural factors
 - Review and collection of documents / electronic evidence
 - Staff interviews
 - Report preparation
 - Identification of opportunities for recovery of loss
 - Control improvements to reduce future losses

Data analysis

- Analysis of large amounts of data through data mining and data analysis
- Data warehouse - repositories of a company's electronic data designed to facilitate reporting and analysis
- Big data - information of extreme size, diversity, and complexity, structured and unstructured
- Structured data – data found in a database, consisting of recognizable and predictable structures
- Unstructured data – without having any predictable structure for e.g. email, word document. For e.g.
 - Social media posts
 - Instant messages
 - Videos
 - Voice files
 - News feeds
 - Sales and marketing material
 - Presentations

Data Mining

- Data mining is the science of searching large volumes of data for patterns. Data mining tools search databases for unclear patterns, finding predictive information that even experts might not recognize. Using data mining technologies, companies can evaluate vast amounts of information, spotting patterns. Data mining can be used for predictive or detective fraud monitoring and investigation. Data mining tools can mine databases for various fraud indicators, such as specific types of transactions; patterns within the data; or a relationship between two data fields that should not have a relationship
- Process of data mining would involve
 - Identification of data sources – structured / unstructured - mainframe, applications, hand held devices, telephone systems, time card, key card systems, emails, voice, video etc
 - Identification of how information is stored – database schema, technical documentation
 - Check that the data is complete and appropriate for analysis

Data analysis

- Data analysis refers to any statistical process used to analyze data and draw conclusions from the findings. data analysis involves running targeted tests on data to identify anomalies
- Data analysis process involved
 - Planning phase
 - Preparation phase
 - Testing and interpretation phase
 - Post-analysis phase

Unstructured Data

- Textual analytics is a method of using software to extract usable information from unstructured text data. Linguistic technologies and statistical techniques—including keywords and scoring algorithms are used to categorize data to reveal patterns, sentiments, and relationships indicative of fraud
- Fraud Keywords – that are likely to point to suspicious activity depending upon the industry, fraud schemes, and the data set etc
 - Pressure – trouble, problem, concern
 - Opportunity – override, adjust, discount
 - Rationalization – deserve, reasonable
- Emotional Tone Analysis – derogatory, surprised, secretive, or worried communications
- Visual Analytics - graphs, heat maps, link diagrams, time-series charts to identify outliers
 - Tree Maps - is a type of heat map in which rectangular space is divided into regions and then each region is divided again for each level in the hierarchy with size and shading representing additional data points
 - Link Analysis - visual representations lines showing connections of data from multiple data sources to demonstrate complex networks; communications, patterns, trends, and relationships for e.g. AML
 - Geospatial analysis – showing intersections between various types of data and its corresponding geographical location for e.g. in insurance claims
 - Timeline analysis – representation across timeline

Digital Forensics

- Digital investigation vs digital forensics
 - Digital investigations are investigations that involve relevant digital data processed or stored by digital devices. Digital investigator need not be forensic examiner
 - Digital forensics encompasses the recovery and investigation of material found in digital devices. Digital forensic experts are individuals who specialize in identifying, recovering, collecting, preserving, processing, and producing digital data for use in investigations and litigation.
- Different types of experts
- Digital evidence - computer, can be a target of a criminal act or an instrument of crime, or a repository of evidence associated with the crime
- Digital evidence – more volatile than tangible information because data can be altered or destroyed more easily than tangible information. Strict forensic methodologies be followed to satisfy the stringent evidentiary standards necessary to ensure the integrity of the evidence beyond a reasonable doubt for presentation in court
- Locating digital evidence

Digital Forensics

- Computer forensics
 - Computer forensics specialists can recover different types of information from computer systems
 - Planning – needs consultations with legal counsel regarding privacy issues. There should be written privacy policies and signed by employees stating that digital resources are solely for business use and that the company reserves the absolute right to review, audit, and disclose all matters sent over the system or placed in storage
 - Seizing –
 - Secure evidence
 - Document the collection process
 - Implement a system to manage the evidence - Search, categorize and distribute digital evidence using tools. The organization can use following to process large amounts of data
 - Analyzing
 - Reporting

Digital Forensics

- Mobile forensics
 - Planning – needs consultations with legal counsel regarding privacy issues
 - Seizing –
 - Extract
 - Analyze evidence
 - Document
 - Report


Interview Process


- Planning for interviews
- Legal considerations
- Conversation elements
- Inhibitors of communication
- Facilitators of communication
- Best practices
- Interview mechanics
- Questioning typology
- Questioning sequence – general to specific
- Questioning techniques
- Dealing with resistance
- Handling resistance
- Handling deception
- Non verbal responses
 - Proxemics – use of interpersonal space to convey the meaning – distance between interviewer and respondent
 - Chronemics – use of timing in interpersonal relations to convey the meaning – pacing of length of pause and speed of speech by interviewer
 - Kinetic – use of body movements to convey the meaning like movement of hands
 - Paralinguistics – use of volume, pitch and voice quality to convey the meaning


Interview Techniques


- Kinseic interviews and interrogations
 - Used by interrogators
 - Based on stress and structured questions to help determine guilt For e.g. question like “What do you think should happen to the criminal”
 - The objective is not getting confession but to determine if the subject is telling truth. Judged from verbal and non verbal responses like self-initiated verbal statements that the interviewee initiates without prompting or nonverbal behavior or body language and observable physiological changes, which includes body positioning movements, eyes, crossed arms etc
- Cognitive interview to bring facts of the case together. Typically used by Police
 - Narrative phase – tell whole story. Reconstruct the circumstances of event. Instruct the Eyewitness to Report everything to the last detail. Constructing the events from different orders. Get the witness to change perspective
 - Ask specific details from the narrative – name, numbers, physical appearance, speech characteristics, any conversation with suspect

Report Structuring

- 
- Background outlining
 - Why the fraud investigation was conducted (e.g., whistle blower complaint, anomaly discovered during an internal audit, occurrence of loss of asset etc).
 - Who called for the investigation and who assembled the investigation team

- 
- Executive outlining
 - What actions were performed during the fraud investigation (reviewing documents, interviewing witnesses, conducting analyses or tests, etc.)
 - The outcome of the investigation – the extent of fraud, how the fraud happened and who is responsible for the loss for e.g. misappropriation of cash of Rs 50,00,000 by the cashier

- 
- Scope outlining
 - The scope of the investigation – for e.g. how the cash was misappropriated, what is the extent of loss and who was responsible for the loss

- 
- Approach outlining
 - Composition of the investigation team
 - Procedures followed (reviewing documents, interviewing witnesses, conducting analyses or tests, etc.)
 - Persons interviewed

Report Structuring

- Findings outlining
 - Details of what occurred, how many cases had anomaly, who was involved, how did they do it, what proof is there etc.
- Summary outlining
 - Results of the fraud investigation - similar to the outcome stated at the end of the Executive Summary
 - Impact for the organization
- Recommendations – this can be a separate document or part of the report. Typically outlining
 - What follow-up action is necessary or recommended, including remedial measures such as a
 - review of internal controls, update of operating guidelines etc
- Annexures and supporting documents
 - Key supporting documents gathered during investigation



Thank You

CA Pradeep Godbole