

# ICPAK FORENSIC AUDIT SEMINAR

*November 2017*



# Introduction



---

## *What is Fraud?*

A word cloud centered around the theme of fraud. The words are of various sizes and colors, arranged in a circular pattern. The most prominent words are 'corruption', 'investigations', 'CAPABILITY', 'cyber', 'FRAUD', 'collusion', 'motivate', 'regulation', 'forensic', 'opportunity', 'capability', 'rationale', 'fraudster', 'theft', 'VALUES & NORMS', and 'rationality'.

## *Introduction to Fraud*

---

“A false representation of a matter of fact, whether by words or by conduct, by false or misleading allegations, or by concealment of that which should have been disclosed, which deceives and is intended to deceive another so that he shall act upon it to his legal injury.” - Black’s Law Dictionary

The five elements of fraud are:

- A representation about a ***material fact***, which is ***false***,
- And made ***intentionally, knowingly***, or ***recklessly***,
- Which if ***believed*** and ***acted*** upon by the victim,
- Can cause the victim’s ***harm*** or ***unfair advantage*** to the perpetrator..

# *Understanding Fraud*

---

## *Understanding Fraud- Fraud related terms*

---

### Error

É Unintentional misstatement in financial statements, including the omission of an amount or a disclosure.

### Irregularities

É Intentional misstatements or omissions in the accounting records or financial statements.

### Wrong doing

É Intentional inappropriate activities such as conflict of interest, gross administrative abuse, misuse of funds or assets, theft, abuse, exceeding or non-compliant with authority thresholds and unethical behavior

### Corruption

É Involves efforts to influence and/or the abuse of public authority through the giving or the acceptance of inducement or illegal reward for undue personal or private advantage.

---

## ***Understanding Fraud- Fraud related terms***

---

### Financial misconduct

É This refers to willful or negligence in fulfilling: general responsibilities; budgetary responsibilities; and reporting responsibilities.

### Allegations

É These are statements of wrongdoing made without proof and can lead to commencement of an investigation.

### Documentary evidence

É This means evidence obtained from documentation that is used to support findings and conclusions emanating from an audit/investigation

### Economic crimes

É This includes crimes against the public, for example corruption and bribery, as well as crimes involving property, for example theft, fraud and forgery.

### Fraud examination

É Refers to a methodology for resolving fraud allegations from inception to disposition.

---

---

## *Understanding Fraud- Fraud related terms*

---

### Investigations

É It's the process of fact finding.

### Fraud risk factors

É Are events or conditions that indicate an incentive or pressure to commit fraud or provide an opportunity to commit fraud.

### Legal forum

É Refers to a forum that provides a medium for the settlement of matters relating to substantive issues of disagreement or legal action between two or more parties.

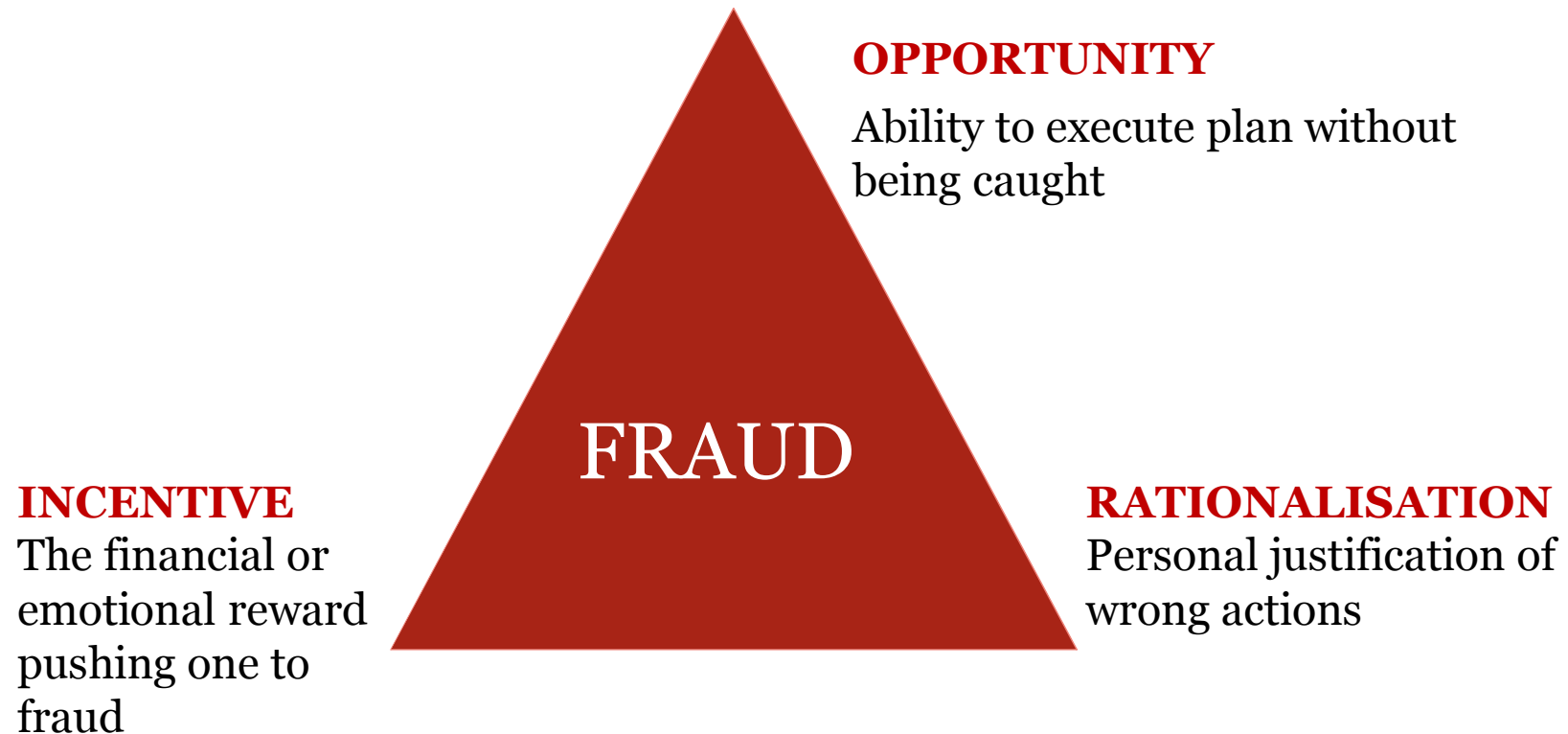
### Money laundering

É this refers to an activity which has, or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities.

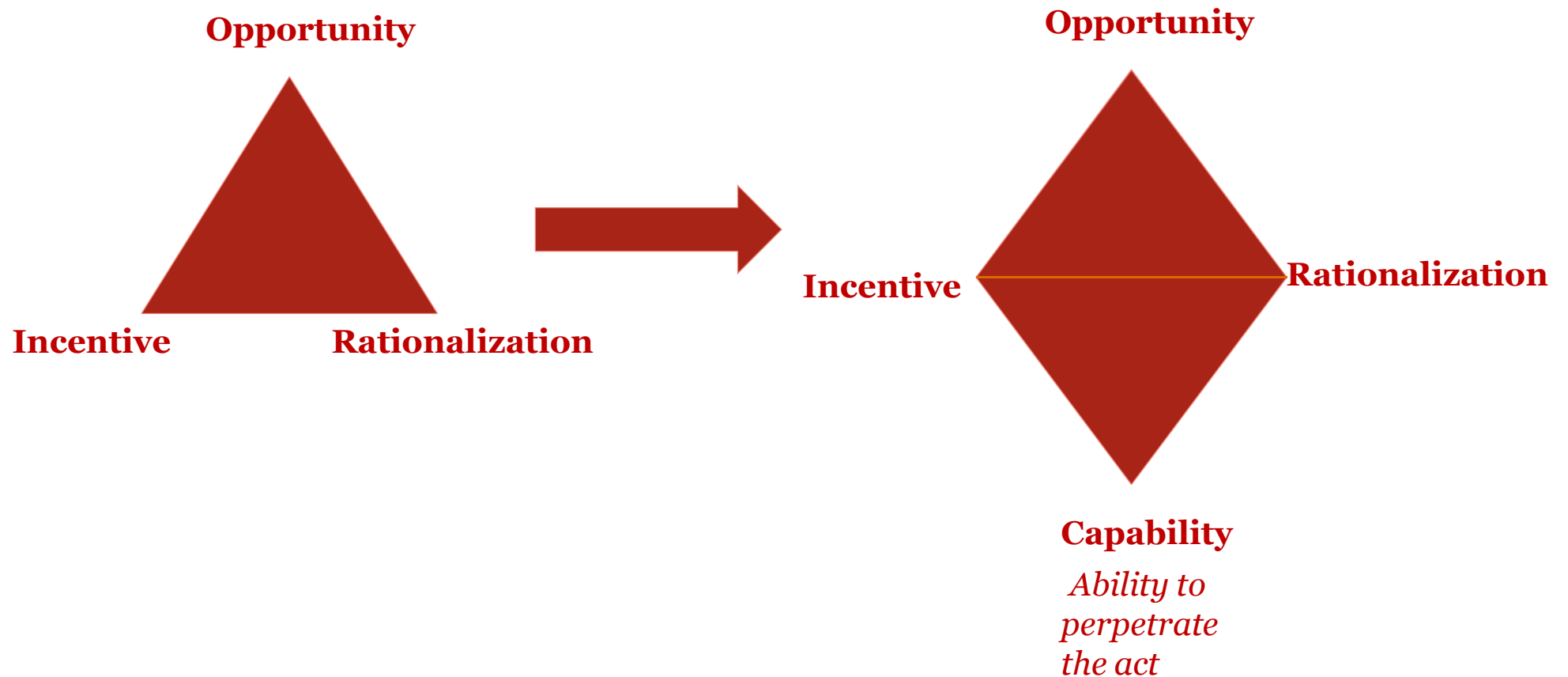


## *The Key Drivers of Fraud: The Fraud Triangle*

---



## *The Key Drivers of Fraud: The fraud diamond*



## ***Forensic Audit Vs Financial Audit***

---

Involves review of information that the organization being audited is ready and willing to provide. May at times uncover fraudulent activity though it's not aimed at achieving this.



Financial  
Audit

Forensic Audit

Involves a review of the information the forensic auditor requires and is not dependent on what the organization is ready to disclose. It does not offer assurance on compliance with GAAP .

# *Profile of a Fraudster*

---

## ***So what is the character of the white collar crime***

---

The ACFE's global fraud study carried out in 2014, was carried on more than 1,400 occupational fraudsters from more than 100 countries. Some of the characteristics are as follows;

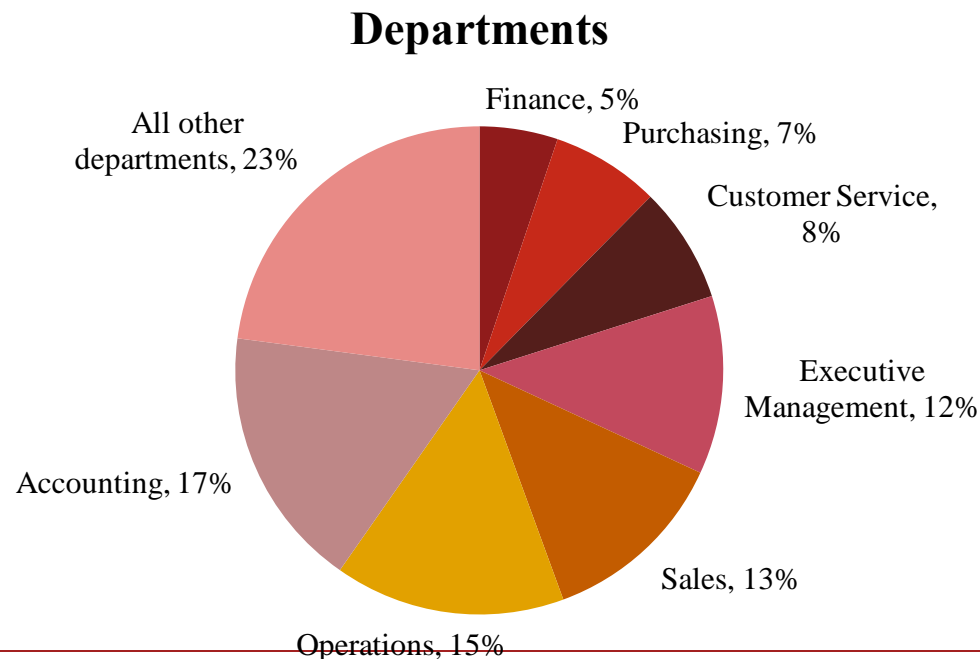
- ❑ Position; the majority of the occupational frauds are committed by staff at the employee and management level i.e 42% = Employees, 36% = Manager and 19% = Owner/Executive;
- ❑ Median loss by position; The higher the fraudsters level of authority the greater the losses tend to be;
- ❑ Gender; Male fraudsters outnumbered the female fraudsters in the ratio of 2:1
- ❑ Median Loss by Gender; Losses attributed to males are 123% higher than those associated to females;
- ❑ 52% of the fraudsters were between the ages of 31 to 45 years old while older fraudsters cause larger losses;

---

## ***So what is the character of the white collar crime***

---

- ❑ 7% of the perpetrators committed fraud in the first year while 53% had worked for at least five years.
- ❑ Median loss by tenure; The longer a fraudster has worked for a company the more the harm he/she is likely to cause;
- ❑ Departments;





---

## *Typical irregularities & red flags*

---

### **Procurement**

- “ Fronting – background checks (supplier database) – Importance of data analytics
- “ Inflated/fictitious invoices – round numbers, thresholds, diluted purchases – importance of trend analysis
- “ Tender rigging – background checks, disclosures, evaluation and adjudication of bids, single sourcing
- “ Service delivery – lack of monitoring (deliberate), inferior quality, incompleteness, scope extensions
- “ Conflict of interest - retail staff having their own shops that also sells phones

### **Human resource**

- “ Ghost employees – staff counts, bank accounts, ancillary staff – data analytics
  - “ Leave – high leave balances (fraudsters do not take leave), leave taken not applied for, abuse of flexible working arrangements
  - “ Remuneration and benefits – bonus/incentive schemes (linked to performance), false reporting
  - “ Expenses – non-official trips, trips with suppliers/customers
-

---

## *Typical irregularities & red flags*

---

### **Information Technology**

- “ Cyber crime – hackers (unauthorised access), access routines (accessing specific databases at certain days/times) – IT pen-tests and data analytics

### **Finance**

- “ Payment approvals – thresholds, delegated authority
- “ Maker-checker controls – initiator and approver are the same (sometimes due to delegated powers)
- “ Reconciliations – suspense accounts, high volumes of transactions

### **Sales & Marketing**

- “ Sales targets – false reporting, periodic hikes, cancelled orders/credit notes
- “ Sales terms – unauthorised discounts, unusual payment terms
- “ Abuse of marketing material and benefits – business trips, business credit cards
- “ Unrecorded sales – cash embezzlement,
- “ Competitions/promotions – collusion with intermediaries/contestants

### **Operations**

- “ Misappropriation of assets – staff vehicles, stationery, internet and other accessories
-

---

## ***Types of Red Flags and Fraud : General Red Flags***

---

### ***Employee Red Flags***

- “ 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
- “ Lack of segregation of duties in the vulnerable area

**What else ?**



---

## ***Types of Red Flags and Fraud : General Red Flags***

---

### ***Management Red Flags***

- “ 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 accounts
  - “ Frequent changes in banking accounts
  - “ Frequent changes in external auditors
  - “ Company assets sold under market value
  - “ Significant downsizing in a healthy market
  - “ Continuous rollover of loans
-

---

## ***Just keep in mind.....***

---

### **Do not ignore a red flag**

Studies of fraud cases consistently show that red flags were present, but were either not recognized or were recognized but not acted upon by anyone. Once a red flag has been noted, someone should take action to investigate the situation and determine if a fraud has been committed.

### **Sometimes an error is just an error**

Red flags should lead to some kind of appropriate action, however, sometimes an error is just an error and no fraud has occurred. You need to be able to recognize the difference and remember that responsibility for follow-up investigation of a red flag should be placed in the hands of a measured and responsible person.

---

# ***Fraud Risk Management***

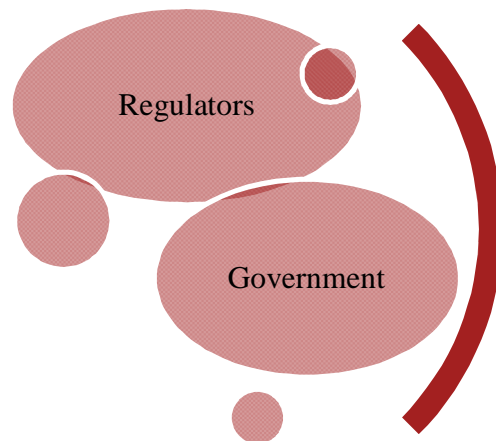


# ***Fraud Risk Management***

---

- ❑ Providing insight into fraud prevention, detection and response.
- ❑ Fraud follows an opportunity and attacks weaknesses. Its important to know where you are vulnerable and how to take control!
- ❑ According to a survey carried out by Deloitte in 2012 on internal audit fraud challenge they observed that FRM is on the rise due to various factors;

Increase in the level of  
scrutiny by



Appearing in form of



Of respondents have  
increased their focus on  
FRM

## ***Fraud Risk Management...Steps***

The continuous plan to diagnose, detect, and respond to fraud would generally include the following steps

| Diagnose vulnerability to Fraud   | Detect gaps in anti fraud controls  | Recommend mitigating anti fraud controls  | Continuous monitoring  | Develop Fraud response plan   | Investigate cases of alleged fraud  |
|---|---|---|--|---|---|
| <ul style="list-style-type: none"><li>É Evaluate current status and effectiveness of anti fraud control environment</li><li>É It includes; culture, attitude, awareness on the knowledge of and response to issues of fraud</li></ul> | <ul style="list-style-type: none"><li>É Evaluate the existing fraud risk management framework to detect potential gaps in the controls and processes</li><li>É Establish the risk profiles and rank them against existing anti fraud controls</li></ul> | <ul style="list-style-type: none"><li>É Recommend enhancement of the existing controls</li><li>É Based on the gaps identified</li></ul> | <ul style="list-style-type: none"><li>É Enable continuous monitoring of controls using the available technology</li><li>É Carry out periodic data analysis to flag any fraud signals</li></ul> | <ul style="list-style-type: none"><li>É This is to respond to cases of alleged or confirmed fraud</li></ul> | <ul style="list-style-type: none"><li>É Consolidate factual findings on the alleged/confirmed fraud</li><li>É Incorporate the identified fraud risks and schemes into the fraud risk management framework</li></ul> |

---

## ***Fraud Risk Management***

---

“To think, we know and understand all risks around us is misleading, to think we can manage all of them, if they hit us, is an illusion, and to turn a blind eye to them is sheer foolishness.”

---