Visualizing Fraud in your Data

Presentation by:

Raymond Bett
CEO, Salaam Technology Limited

Thursday, 28th November 2019

CPA Raymond Bett

- Founder and CEO of Salaam Technology Limited.
- Over 10 years Information Assurance, cybersecurity, Forensics, ICT Audit
- Holder of BSC in Electrical and Information Engineering, Cybersecurity Fundamentals CSX, CISA, CISM, CRISC, CEH, CPA Certifications
- President of the ISACA Kenya Chapter, Member of ICPAK and EC-Council.
- Previously worked for Safaricom Limited and PricewaterhouseCoopers (PwC)

The Human Mind – Emotions that are being Exploited

01

Trust

You trust the technical expert with your user credentials to confidential data assets

02

Desire

It is the dangerous desire of helping a stranger tailgate into restricted premises, not knowing their ulterior motives

03

Curiosity

The inquisitive mind in each one of us to open that malicious attachment or CD placed on our desks, with lucrative labels like “” CONFIDENTIAL” or “PAYROLL”

04

Ignorance

Employees in an enterprise being ignorant of clear desk policy or sticking passwords notes on their desks

05

Carelessness

Carelessly dumping confidential documents and password notes into dustbins and leaving laptops unlocked for long intervals

06

Fear Factor

A pop-up window that requests users to re-enter credentials (due to an apparent server error) can be captured, failing to which the active session may be lost

Fraud Basics

Fraud, in the simplest form, is **intentional deception** or misuse of resources for personal gain and/or **resulting in a loss or potential loss** for another entity.

Element of fraud

Big data requires high performance analytics to process billions of rows.

- Misrepresentation of facts by a body.
- Intention to deceive the target by the party submitting the facts.
- The act is unlawful
- A loss or potential loss was suffered.

Common categories of occupational fraud: **corruption, asset misappropriation** and **fraudulent financial statements.**

Fraud Basics

Fraud, in the simplest form, is **intentional deception** or misuse of resources for personal gain and/or **resulting in a loss or potential loss** for another entity.

Element of fraud

Big data requires high performance analytics to process billions of rows.

- Misrepresentation of facts by a body.
- Intention to deceive the target by the party submitting the facts.
- The act is unlawful
- A loss or potential loss was suffered.

Common categories of occupational fraud: **corruption, asset misappropriation** and **fraudulent financial statements.**

Fraud indicators

Indicators of possible fraudulent activities

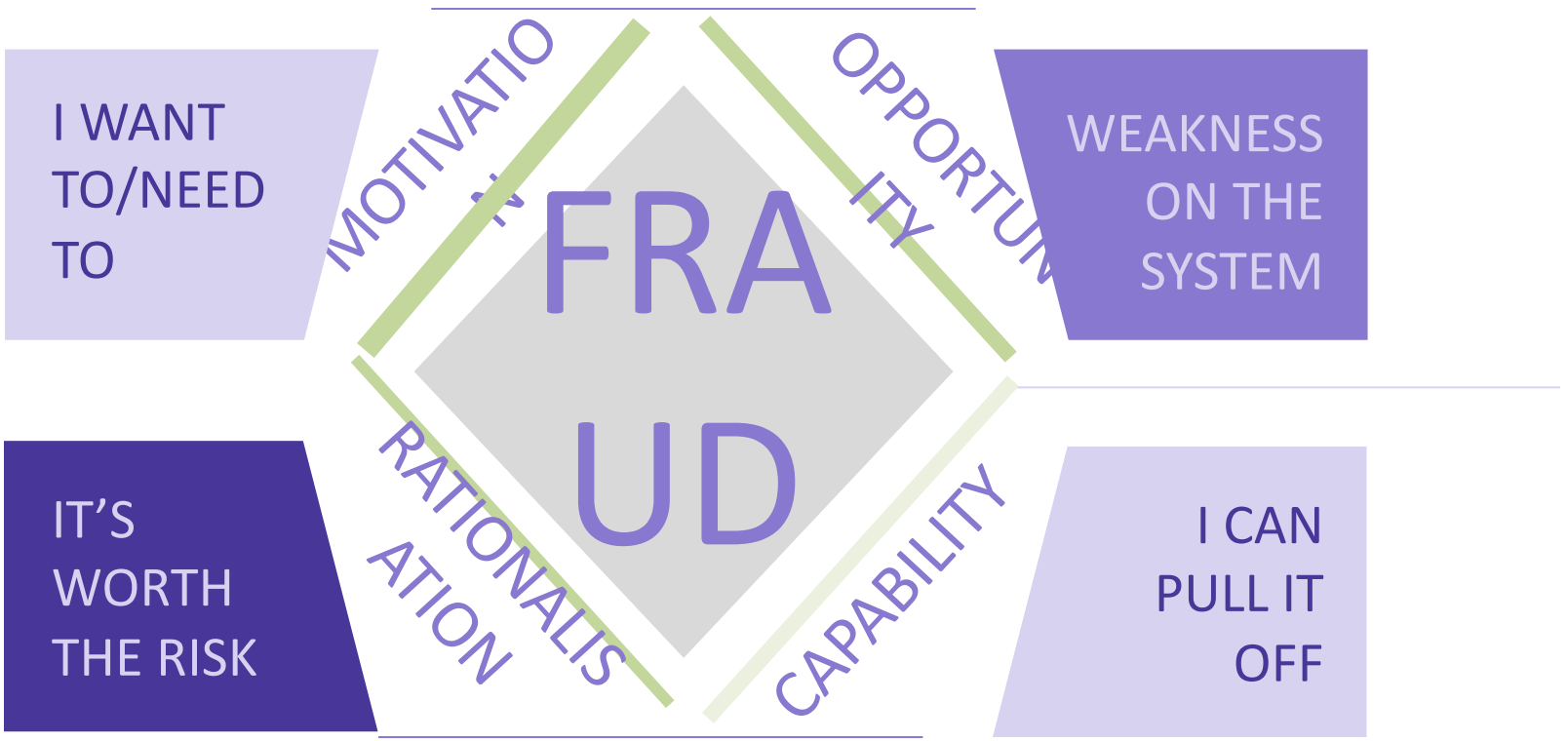
Odd transactions	• Timing of transactions • Value of amounts • Frequency of transactions • Parties engaging in transactions
Employee characteristics	• Motivation • Morale • Job satisfaction levels

Classification of fraud

Indicators of possible fraudulent activities

Odd transactions	• Timing of transactions • Value of amounts • Frequency of transactions • Parties engaging in transactions
Employee characteristics	• Motivation • Morale • Job satisfaction levels

Why fraud occurs



Why fraud occurs

Fraud occurs due to the following:

Motive/ Incentive

Business pressures such as:

- Pressure to reach targets, meet bonus targets
- Pressure to maintain job or promotion path
- Pressure to prop up an ailing parts of group or weak contracts
- Pressure to get new funding

Personal pressures such as:

- Financial problems, divorce or extravagant life style
- Drug or gambling habits
- Greed

Opportunity

- Access to valuable and portable assets susceptible to misappropriation
  - Inadequate focus on internal controls and fraud risk & Poor physical controls
  - Inadequate management oversight of employees
  - Inadequate segregation of duties or independent review Lack of fraud awareness and weakness in ethical culture.

Why fraud occurs

Rationale

- **Reduced remuneration** – My salary has been reduced but I have been performing well.
- **Interest free borrowing** – I will return the money before anybody notices.
- **Group psychology** – Everyone is doing it, so why shouldn't I
- **Personal debt** – I have to pay back my debt or else they shall harm me.
- **Personal Growth** – All my friends have more money than I. I have to show them.

Why fraud occurs

Opportunity

- Access to valuable and portable assets susceptible to misappropriation
- Inadequate focus on internal controls and fraud risk
  - Inadequate management oversight of employees
  - Inadequate segregation of duties or independent review
  - Poor physical controls
  - Lack of fraud awareness and weakness in ethical culture

Capability

- Appropriate skills sets to pull off the fraud.
- Domineering leadership (staff don't question your decisions).
- Understands the control environment
- Trusted individuals

Profile of a fraudster

- Male, 36 to 45 years old
- Employed by the company for more than 10 years
- Holds a senior position
- Works in finance or a finance related role
- Commits fraud against employer and often works in collusion with another perpetrator

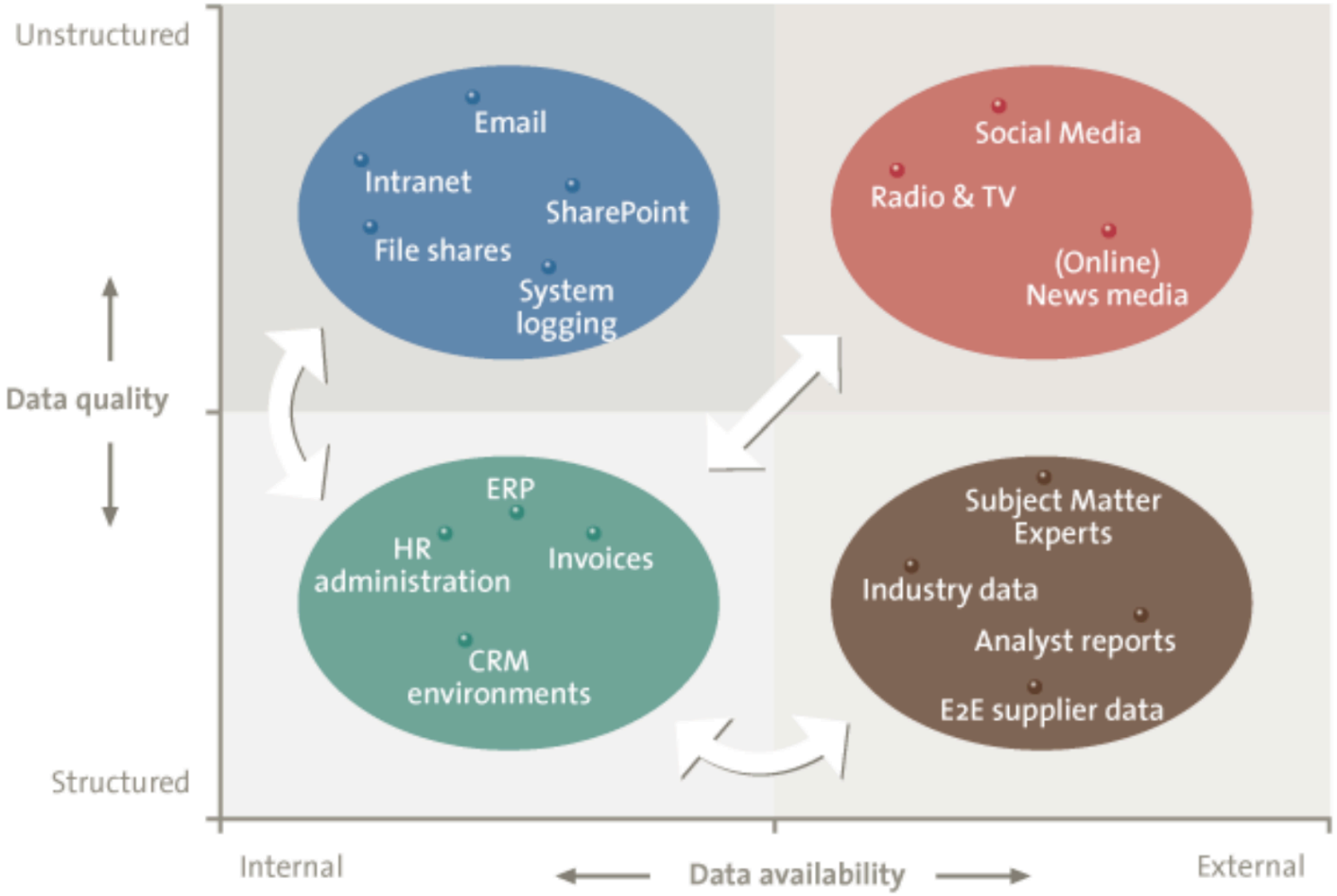
Profile of a cyber fraudster

- Tend to be young
- Less years of service
- More likely to act alone
- More likely to have a sophisticated modus operandi
- More likely to have conducted the fraud over shorter span. (83% less than one year)

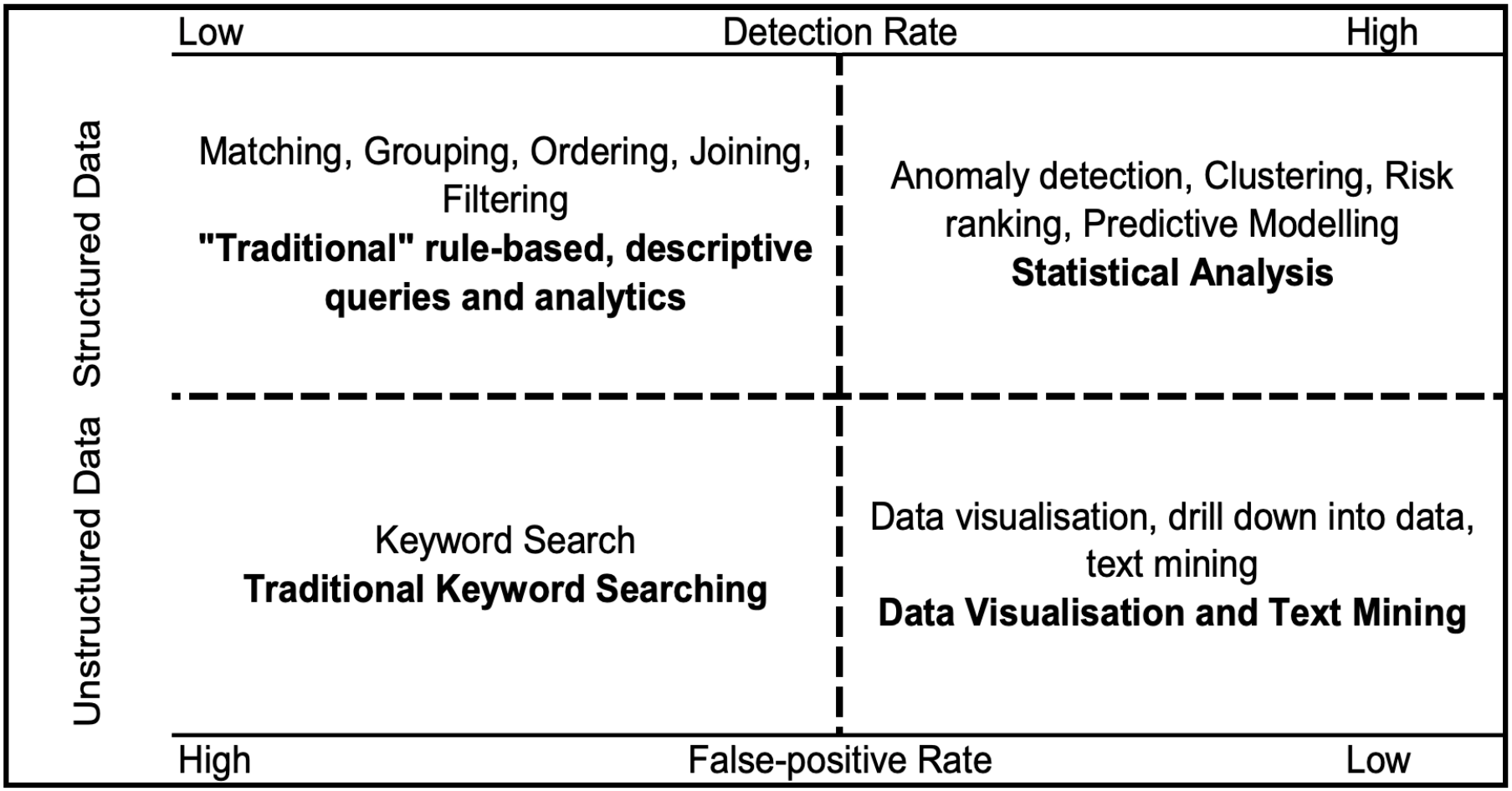
Data Analytics

- Data analytics is useful for:
  - Trend analysis
  - Non statistical predictive modelling
- Regression analysis Supports other testing by providing evidence over:
  - Data extraction for reports
  - Physical access controls
  - Segregation of duties
  - Reliability of data Checks and re-performance require a thorough understanding of the accounting systems in place

Forensic Audits and Data



Forensic Audits and Data



Forensics Red Flags

Expenditure

1. **Unsupported expenditure** – Payment vouchers and other supporting documentation not provided. Reason for expenditure therefore cannot be ascertained.
2. **Excluded expenditure** – total expenditure registered against votes is understated as a result.
3. **Weak or inadequate control over Imprests** – long outstanding imprests amounts. Misuse of imprest process - Procurement of services i.e. training facilities via imprests instead of procurement process (quotations not sourced, lack of market price comparisons)
4. **Irregular payment in allowances** e.g. to individuals who attend meetings they are not supposed to be attending or scheduling meetings that have not been duly constituted
5. **Nugatory expenditure** – This is expenditure that does not achieve any result e.g. payment for office rent for offices that are yet to be occupied.
6. **Lack of valuation reports for large asset purchases** such as land or property. In other instances, existing valuation reports are not done by government or professional valuer.
7. **Contracted companies enter into MOU's with private firms** who perform all the associated work
8. **Unexplained under-expenditure** – Expense amount far less than budgeted amount.
9. **Unexplained expenditure increases** – Year to year show a significant increase in expenditure.
10. **Unsupported disbursements** – Bank certificates and documentary evidence of work carried out not provided.

Forensics Red Flags

Finance and Budgeting

1. Poor maintenance of accounting records - For instance, various ledgers and trial balances against which the financial statements are drawn found to be incomplete, not up to date, or totally missing. In other instances, routine below-the-line accounts not analysed to indicate what they represented. Material book-keeping errors detected in various records.
2. Failure to keep minutes of meetings or presence of unsigned minutes –
3. Opening of new bank accounts without approval from authorities such as Treasury
4. Significant increase in Tax payable from previous year – No tax computations provided to show computation of tax.
5. Miscellaneous income – Nature and description of miscellaneous income not defined or explained.
6. Lack of bank reconciliations – Several bank statements without reconciliation data. In some cases; missing bank statements.
7. Ageing Analysis report (Long outstanding debts) – long outstanding debtors with inadequate or ineffective debt collection measures.
8. Exchange rate difference
9. Missing fixed assets register – necessary for confirmation of asset ownership status, purchases and disposals.
10. Variances between receipt books and control records – Records show less receipt books issued to the revenue collection department as compared to the number of receipts books used.

Forensics Red Flags

Finance and Budgeting

11. Long outstanding Stale cheques and unrecorded receipts
12. Unsupported bank transactions – Withdrawals made from bank yet supporting documents to demonstrate who was being paid and reason for payment
13. Discrepancies in loan records and unsupported loan balances
14. Inaccurate financial statements – Discrepancies between entries in Statement of Financial assets, statement of cash flows etc.

HR and Payroll

1. Irregular payments – I.e. Payroll: Pension overpayments and reason provided due to erroneous multiple payments to the pensioners.
2. Lack of HR Policy - Failure to develop a Human Resource and Training Policies that prescribe the procedures to be followed.
3. Selectively accelerated promotions - basis of acceleration not clearly indicated
4. Appointment of staff without obtaining necessary approvals.
5. Unrecovered Salary advances – Salary advanced to employees are not recovered at the end of the period.
6. Staff in acting capacity for more than 6 months – No review made by the CEO/Director to extend this period.

Forensics Red Flags

Finance and Budgeting

11. Long outstanding Stale cheques and unrecorded receipts
12. Unsupported bank transactions – Withdrawals made from bank yet supporting documents to demonstrate who was being paid and reason for payment
13. Discrepancies in loan records and unsupported loan balances
14. Inaccurate financial statements – Discrepancies between entries in Statement of Financial assets, statement of cash flows etc.

HR and Payroll

1. Irregular payments – I.e. Payroll: Pension overpayments and reason provided due to erroneous multiple payments to the pensioners.
2. Lack of HR Policy - Failure to develop a Human Resource and Training Policies that prescribe the procedures to be followed.
3. Selectively accelerated promotions - basis of acceleration not clearly indicated
4. Appointment of staff without obtaining necessary approvals.
5. Unrecovered Salary advances – Salary advanced to employees are not recovered at the end of the period.
6. Staff in acting capacity for more than 6 months – No review made by the CEO/Director to extend this period.

Forensics Red Flags

Procure to Pay

1. Direct procurement – Companies directly contracted without a valid justification instead of following the public procurement procedures i.e. Public participation.
2. Missing approval of payments to suppliers – Approvals for payment of suppliers not approved by proper authorities.
3. Unsupported Purchases – Lack of Purchase orders, invoices/ receipts.
4. Poor records maintenance – Non-maintenance of individual project files for each procurement requirement complete with a reference number.
5. Lack of inspection reports for completed projects
6. Delays in execution of contracts
7. Change of contract terms at signing stage e.g. initially agree on fee inclusive of VAT but contract is signed as exclusive of VAT.
8. Goods and Services that are never supplied – No evidence of supply
9. Projects under work-in-progress status for long period
10. Contract award to unqualified bidders
11. Inadequate due diligence on performance bank guarantees – especially those issued by foreign banks
12. Inadequate or no vetting of bidders

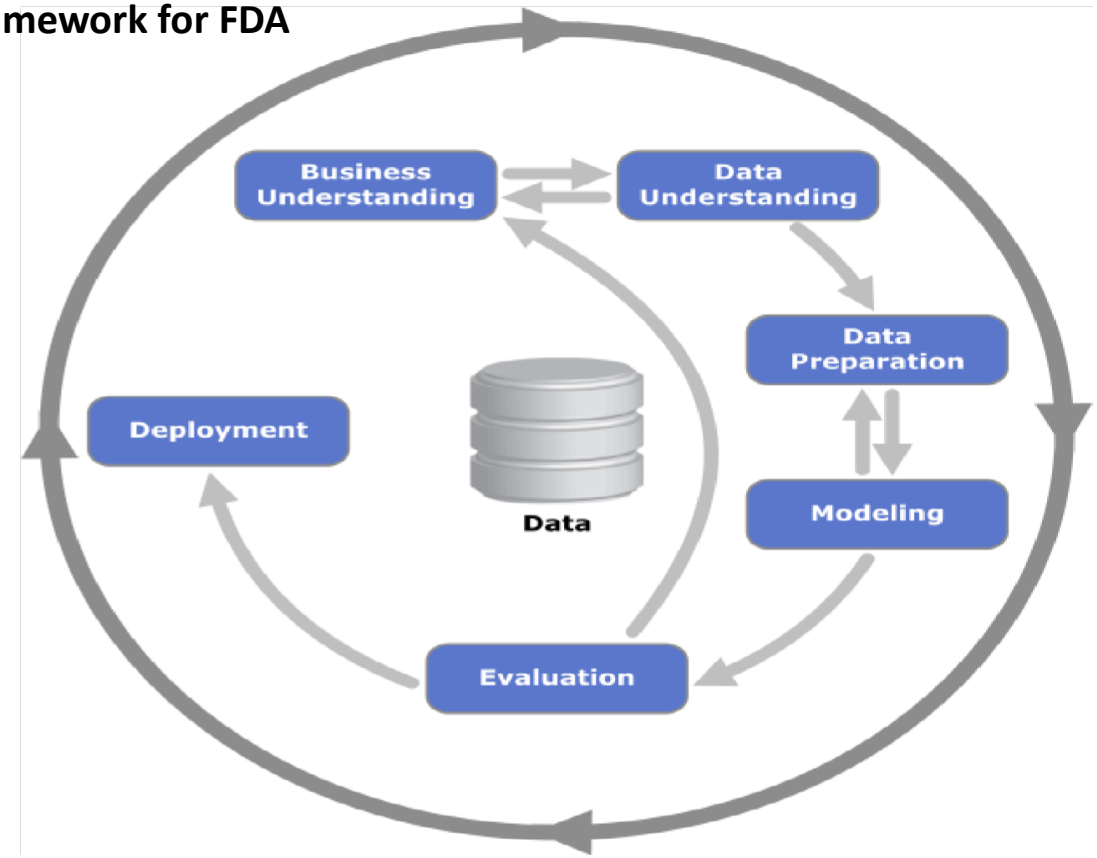
Forensics Red Flags

Procure to Pay

1. Direct procurement – Companies directly contracted without a valid justification instead of following the public procurement procedures i.e. Public participation.
2. Missing approval of payments to suppliers – Approvals for payment of suppliers not approved by proper authorities.
3. Unsupported Purchases – Lack of Purchase orders, invoices/ receipts.
4. Poor records maintenance – Non-maintenance of individual project files for each procurement requirement complete with a reference number.
5. Lack of inspection reports for completed projects
6. Delays in execution of contracts
7. Change of contract terms at signing stage e.g. initially agree on fee inclusive of VAT but contract is signed as exclusive of VAT.
8. Goods and Services that are never supplied – No evidence of supply
9. Projects under work-in-progress status for long period
10. Contract award to unqualified bidders
11. Inadequate due diligence on performance bank guarantees – especially those issued by foreign banks
12. Inadequate or no vetting of bidders

Forensic Data Analysis.

A General Framework for FDA



Forensic Data Analysis.

1. Business understanding
This initial phase focuses on understanding the project objectives and requirements from a business perspective, and then converting this knowledge into a data mining problem definition, and a preliminary plan designed to achieve the objectives.

2. Data understanding
The data understanding phase starts with an initial data collection and proceeds with activities in order to get familiar with the data, to identify data quality problems, to discover first insights into the data, or to detect interesting subsets to form hypotheses for hidden information.

3. Data preparation
The data preparation phase covers all activities to construct the final data set (data that will be fed into the modeling tools) from the initial raw data. Data preparation tasks are likely to be performed multiple times and not in any prescribed order. Tasks include table, record, and attribute selection as well as transformation and cleaning of data for modeling tools.

A General Framework for FDA

4. Modeling

In this phase, various modeling techniques are selected and applied, and their parameters are calibrated to our estimated optimal values.

Typically, there are several techniques for the same data mining problem type. Some techniques have specific requirements for the form of data. Therefore, stepping back to the data preparation phase is often necessary.

5. Evaluation

At this stage in the project you have built a model (or models) that appear to have high quality, from a data analysis perspective.

Before proceeding to final deployment of the model, it is important to more thoroughly evaluate the model and review the steps executed to construct the model, to be certain it properly achieves the business objectives.

A key objective is to determine if there is some important business issue that has not been sufficiently considered. At the end of this phase, a decision on the use of the data mining results should be reached

A General Framework for FDA

6. Deployment

Creation of the model is generally not the end of the project. Even if the purpose of the model is to increase knowledge of the data, the knowledge gained will need to be organized and presented in a way that the client can use. Depending on the requirements, the deployment phase can be as simple as generating a report or as complex as implementing a repeatable data mining process. In many cases it will be the client, not the data analyst, who will carry out the deployment steps. However, even if the analyst will not carry out the deployment effort, it is important for the client to understand up front the actions which will need to be carried out in order to actually make use of the created models.

Application of FDA

Fraud Risk and Compliance

- Fraud Detection and Risk Management
- Regulatory Proceedings
- Bribery and Corruption
- Asset Misappropriation
- Competition Law
- Quantum Loss Estimation
- Transaction due diligence
- Financial Crime
- Corporate Restructuring
- Third party due diligence

Customizable Business Processes

- E-payment Systems
- Sales and Marketing
- Ecommerce
- Procure to pay
- Time and Expense
- Human Resources
- Multi Data Acquisition
- Automated data mining
- Investigative data linking
- Social network analysis
- Data visualization
- Statistical inference
- Artificial intelligence
- Programming and decision support

Application of FDA

Business Area	Examples of Analytical Tests
Manual Journals: Highlighting unusual journals and patterns to obtain an overview of key internal control risks for follow up	• Identify users that are posting journals without authorisation • Identify postings on public holidays or out of office hours • Identify all out of balance entries
Payroll: Profiling and analysis of payroll transactions and records for fraud, waste and abuse	• Identification of changes in base salary that have occurred outside usual period • Identification of duplicate bank accounts details • Payments to individuals that are not on the Payroll Register • Check employees, contractors against watch lists such as Political Exposed Persons
Procurement: Profiling and insights into the Accounts Payable department including regulatory, fraud and internal control issues	• Analysis payments to "one-time" vendors or vendors not found on the vendor master file. • Duplicate Payments Analysis • Identify overcharging by contractors by comparing total value shown on the contract to the sum of the line item subtotals • Identify PO's which have changed by 10% more than their original value
Expenses: Identifying expense misuse and purchases not in accordance with the company policy	• Identify employees claiming more than 3 times the average annual claim per grade • Identify employees making hotel claims over the agreed monetary threshold per grade • Identify instances when employees have not requested the company rate
Systems/Application Access: Identifying breaches of system and Application access controls	• Application based view of access logs focussing on leave and join dates • List of dormant privileged users on an application basis • Data profiling of privileged access/super user activities • Profile of access categories and comparison with log profiling and controls in place

Forensic Data Analysis Techniques

Technique	Description
Even amounts	In this technique the investigator identifies even dollar amounts, numbers that have been rounded up, such as $200.00 or $5,000.00. The existence of even amounts may be a symptom of possible fraud and should be examined.
Ration analysis	Like financial ratios that give indications of the relative health of a company, data analysis ratios point to possible symptoms of fraud. Three commonly employed ratios are: Maximum/minimum; maximum/2nd highest; and current year to the previous year. A large ratio could indicate an anomaly in the data and unexplained deviations could be symptoms of fraud.
Trend analysis	Analysis of trends across years, departments, or other parameters can be very useful in detecting possible frauds. Another useful calculation is the ratio of the current year to the previous year where a high ratio indicates a significant change in the totals.
Benford's law	Benford's Law calculates the expected frequencies (rounded to three decimal places) for first and second digits. It concludes that the first digit in a large number of transactions (10,000 plus) will be a '1' more often than a '2'; and a '2' more often than a '3' hence a deviation from this expectation should be investigated.

Key takeaways

Technology is changing – more emphasis on data driven audits

Demand for automation – cyber risks have emerged

To deliver a comprehensive audit, auditors need to enhance their data analytics skills

Need for collaboration – auditors and audit committee level. Also, understand affecting regulations

About Salaam Technology

Salaam Technology is a Kenyan ICT firm whose ***mission*** *to be at the forefront of securing digital networks for our clients through differentiated products and services that ensures a safer and a secure cyberspace*

Salaam Assurance

- An independent audit on IT governance, access to programs and data, computer operations and interfaces. We provide assurance before you carry out any major systems changes or immediately thereafter or even through an annual compliance cycle. This can be on ICT audits or vulnerability assessment and penetration testing

Salaam Awareness

- We provide training and awareness on various emerging areas on IT such as Cybersecurity, Forensics etc. We have partnered with the leading providers of this platform such as KnowBe4 among others.

Salaam Managed Services

- Given our expertise in inspecting various security products, talk to us if you need any product or service relating to cybersecurity be it firewalls, antimalware products, encryption certificates or anything in between. Our Managed cybersecurity offering will ensure that we partner together to achieve a cyber resilient organization. With our expertise in incident response, we are sure to provide the best in class service as we hunt the malicious actors detect attacks and respond to them before they escalate

Questions?

Raymond Bett

M-PESA, Whatsapp,
Truecaller, +254 720 983 411
raymond.bett@salaam.ke

www.salaam.ke