# GUIDE TO DATA MINING AS A TOOL IN FRAUD INVESTIGATION

Introduction/FOREWORD

Fraud poses to the auditor an unavoidable risk that some material misstatements of the financial statements may not be detected (ISA240).

The guide is designed to assist the auditor twofold namely in reactive- and proactive analysis (Fraud examiners Manual).

Reactive analysis will assist an auditor to make use of data analytics in the event of fraud being detected which is covered in Section 1 of the guide. Section 1 sets about the data analytic process to be followed when reacting to committed fraud and allows the auditor to fully assess and quantify the impact/ extent of the perpetrated fraud should a computer system have been used.

Proactive analysis covered in Section 2 of the guide will assist auditors in fraud risk determination as part of their annual audits, i.e. making use of data analytics to predict/ indicate the presence of possible fraud in the pursuit of the auditor to gain assurance on financial misstatement due to fraud.

The prevalence or at least the likelihood of fraud will be assessed by collating analytically identified fraud risk indicators with a fraud scoring model. The fraud scoring model forms the basis by which the auditor will be able to form an opinion over the fraud risk he/she is exposed to within the audit engagement.

Section 3 of the guide explores step-by-step the design of an analytical solution incorporating the fraud scoring model to automate the data mining of fraud indicators yielding a fraud risk profile of the audit engagement. The fraud indicators used is derived from commonly known fraud practises as well as audit procedures used to detect these. The Annexure to the guide provides an overview of known schemes and the auditor's response to it whereas the solution charts the implementation thereof analytically.

Decision to perform reactive analysis

It is important for the auditor to understand when data mining is to be applied in assisting the fraud investigator. Often auditors wants to make use of data analysis but the fraud/ corruption was not perpetrated making use of the system. Data analysis has the fundamental requirement that data is needed and if the fraud is not in the system no data mining can be achieved.

It is thus important for the auditor to consider before approaching the data analyst whether the fraud perpetrated or the fraud/ corruption scheme involved the computer system. A minimum of one fraud element/ action should have been perpetrated in the system which would allow the data analyst to support the fraud investigation.

Fraud defined

ISA 240 defines fraud as *"An intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage."*

The Association of Certified Fraud Examiners (ACFE) defines occupational fraud as "*The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or asset".* The ACFE classifies occupational fraud into three categories:

- Asset misappropriation
- Financial statement fraud; and
- Corruption

ISA 240 does not concern itself with corruption but from a public sector perspective corruption is a concern of the auditor in conjunction focussing on misstatements in the financial statements arising from either fraud or error. Distinguishing between fraud and error is whether the underlying action that results in the misstatement of the financial statements is intentional or not. (ISA 240)

***Asset misappropriation*** refers to the theft of assets (cash/inventory/other) and fraudulent disbursements. The theft of assets is not fraud but the action to cover the theft normally leads to fraud being committed in the forms of "*sophisticated and carefully organised schemes designed to conceal it*" (ISA 240). Examples of asset misappropriation are:

- Cash sales not recorded and pocketing the money
- Skimming of cash and lapping thereof
- Write-offs – disposing of new assets concealed as old

ISA 240 states "*Management is in a unique position to perpetrate fraud because of management's ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively.*"

In this sense ***financial statement fraud*** pertains to the deliberate manipulation of the financial statements resulting in overstatements (assets/income) or understatements (liabilities/expenses). Examples of financial statement fraud are:

- Inflated revenue
- Timing differences – cut off
- Improper valuations

***Corruption*** pertains to instances where the employee benefits himself/herself over the best interests of the organisation. ACFE states corruptive behaviour as *"the offering of anything of value to influence the action of another."* Thus the employee uses his/her position to gain financial benefit directly or indirectly by accepting or insisting on payment (money/ otherwise) to act unethically. Examples of corruption are:

- Conflict of interest – allocation of purchases to employee/ family member owned company
- Purchasing schemes – overbilling or billing for fictitious inventory
- Invoice kickbacks – favouritism towards certain suppliers

# Section 1 – Reactive analytics

Discovered fraud analytics

It is often perceived that committing fraud through the use of computers is highly complex and difficult to trace. A clear distinction should be made when computer fraud is being perpetrated by a system user or by a malicious attacker such as hackers.

A hacker gain unauthorised access to your confidential system through unethical intrusive and brute force methods whilst the internal employee has access and abuses their authority. In abusing the responsibility and authority given to employees the employee will not employ "hacker" type methods. The employee will identify gaps in the system or controls and exploit these to their benefit. The fraud will be perpetrated by using the system to gain the desired benefit or capture the already designed manual fraud into the system.

When utilising data analytics to assist the fraud investigation said fraud scheme has been uncovered whereas the objective of the investigation is to ascertain the impact the scheme had in terms of financial loss and financial statement disclosure.

Analytical approach to discover extent (quantifiable action)

The objective of the auditor when fraud has been uncovered is to respond appropriately (ISA 240, par 10c) meaning the auditor will have to assess the perpetrated fraud by designing and executing audit procedures as part of his/her response. The response will most likely include making use of specialists/ experts such as a fraud investigator and data analyst.

The role of the data analyst will be to assist both the auditor and fraud investigator to obtain and analyse any data to substantively assess the perpetrated fraud. In doing so the data analyst will apply a data analysis process in order to ensure accurate and meaningful results.

The data analysis process is as follows:

- Planning phase
  - Identify the audit objectives
  - Locating the data
  - Identify the relevant data

- Preparation phase
  - Obtain the data
  - Access the data
  - Verify the data

- Design, testing and interpretation phase
  - Transpose audit procedures into data analytical audit procedures
  - Perform the analytical procedures
  - Review and interpret the results

## PLANNING

Identify the audit objective

Data analytics has a multitude of objectives but central to it all is the support that the data analyst provides through data mining techniques. For the purpose of this guide the data analyst has the audit objective to analyse the impact a fraud scheme had in terms of financial loss and financial statement disclosure.

This objective remains the same regardless of the fraud scheme perpetrated.

Locating the data

The data analyst should fully comprehend the system environment within which the fraud was perpetrated. The data analyst must know the type of data that is to be analysed and how the data is structured and the transaction flow throughout the system.

The data analyst source of information about the financial system in place will be best addressed by a combination of ICT and the system owners. ICT will be able to provide the technical platform and infrastructure of which the database administrator will be most useful. The system owners will provide information on how transactions are processed in the system and the system programmers within ICT will assist to relate data tables, fields and rules of the system from a technical specification.

The data analyst should have covered the following at minimum:

- Blueprint of the system – overview of all modules of the system and the interface points between each module
- How data is stored
- What data is stored
- How the system processes transactions
- How accounting system works
- Where is the detail stored for example in the general ledger or sub ledger
- What other system carried history information is available

*NB! The data analyst will always need detail of transactions and not rolled up transactions*

Identify the relevant data

The data analyst will study the fraud scheme and break it down into its fundamental elements in terms of data representation. The data analyst will also consider the full transaction flow through the system considering how the fraud scheme works and determine system pointers/ parameters that would assist in identifying committed fraudulent transactions.

The data analyst's main source of information is the data dictionary.

A data dictionary explains each and very field within data tables. The dictionary will indicate the following:

- Field name as it appears in the database; e.g. INIT
- Explanatory field name if abbreviated in the database; e.g. Initials
- The data type of the field, i.e. text, numerical, logical, date; etc.
- Length of the field
- Specific formats of the field, e.g. date = “yyyymmdd”
- The content of the field, purpose of the field in terms of what it carries; e.g. the initials of the employee
- Data flag/ indicator definitions; e.g. M = Male
- Reference key fields that points to other data tables; e.g. employee number

## PREPARATION

Obtain the data

The auditor should submit a formal request for data whether or not a data extract will be provided. Instances where the data analyst will extract the data in person also require permission from the auditee to gain access to the system thus the letter of request will detail such in this event.

When requesting data it is important for the data analyst to consider the format in which the data is to be received considering the abilities of the software tool to be used. The data analytic software needs to be able to read the data files received thus when requesting a data extract the data format has to meet the software specifications. Different formats may also change the representation of data for example personnel numbers are defined and recorded on the system as a text data type but if provided in Microsoft Excel the data type is now numeric meaning that integrity can be lost. For example, personnel numbers are recorded in the database in an alpha numeric text field which can be preceded by a “0” but in a true numeric field the “0” is lost; “0155” vs “155”).

The data analyst should weigh up the best suitable data format given the analytic software, the financial system reports, the database in use and the skills of ICT.

Popular and proven data formats that the data analyst can consider in order of reliability and ease of use:

- Direct access via ODBC
- Flat files
- Delimited files
- Microsoft database
- Microsoft Excel
- Report/ print image files

The formal request for data should stipulate the exact data requirements covering the following:

- The system from which the data is required
- The financial period(s) for which the data is required
- Which tables are needed
- The record layout of the downloaded tables
- The format in which the data is required
- The provision of control totals per data file specifying the number of records and hash totals of numeric fields
- The method and medium of receiving the data
- The extraction scripts used to extract the data
- Expected date for receiving the data

Access the data

Once the data analyst has received the data as stipulated in the request the data analyst will read the data with the data analytic software tool. This usually involves importing/ uploading the data into the software tool.

This step basically converts the data received from a raw state into user friendly data/ information. The data analyst will use the record layouts to structure the data into understandable terms by adding headings and other parameters such as date formats. The data access process is unique to each software tool in which the data analyst will have been trained and will apply his skill in this respect.

Verify the data

Before using the data for any analysis the data analyst will perform validation tests to confirm the integrity of the data including the completeness thereof.

Data validation tests that the data analysts can apply is as follows:

- Verify the data types against the record layout and data dictionary; e.g. text fields are text
- Confirm the record count with the control totals received
- Confirm the hash totals of numeric fields with the control totals received
- Identifying missing data; e.g. blank fields, sequence gaps
- Checking for duplicate data; should there be identified confirm whether it is false positives or not
- Reconcile the data to accounting records such as the trial balance
- Perform reasonability tests such as number of transactions per month. It is reasonably expected that a certain trend exist per type of transaction, etc.
- Perform period testing, i.e. does the data cover the requested period

It should be noted that it is not required to perform all the validations tests but only enough that will give the data analyst assurance surrounding the completeness and integrity of the data received. Any discrepancies identified should be addressed before continuing with analysis. This may include re-requesting the data.

## DESIGN, TESTING AND INTERPRETATION

Transpose audit procedures into data analytical audit procedures

The data analyst has until this point gathered an environmental understanding of the fraud scheme which for the fraud auditor manifested into audit procedures. These audit procedures were the main drivers behind acquiring data sets from the financial and other information systems. The data analyst will now apply analytic audit procedures to isolate/ identify and determine the impact a fraud scheme had in terms of financial loss and financial statement disclosure.

The data analytic audit procedures which can be performed are as follows:

- Compare – find similarities or not between data/transactions from different sources
- Evaluate – test transactions against specific criteria/ parameters
- Duplicate testing – identify duplicate transactions
- Sequence checking – identify missing transactions
- Matching – the use of reference data to identify transactions
- Analyse – the use of statistics and trends to identify anomalies
- Relationship detection – find other transactions similar to ones already identified
- Calculate – recalculate values according set rules and test against recorded transaction values
- Select/stratify – focus on a sub dataset
- Summarise – determination of overall values (totalling)
- Reconciliation – confirming that the collective is fully represented by the parts it's made up of, i.e. completeness of data/ information

Perform the analytical procedures

All analytical procedures involve the use of a software tool to arrive at an answer. The software tool will subject the data according set instructions received from the data analysts. These set instructions are the technical commands used for the tool to apply on the data to isolate or test the data to identify all transactions that reflect the associated system manipulation by the fraudster.

The data analyst will use a single or a series of commands to reach the analytical audit procedures objectives. These commands are unique to each software tool and the data analyst the will have been trained and will apply his skill in this respect. Every command also requires the specific test criteria/ parameter to be applied correctly. The test criterion is program logical expressions that will filter the data to the desired results. For example, the fraud was committed on a specific date thus meaning the data analyst will start of by identifying on the date field all transactions that took place on said date.

Important aspects to keep in mind when performing logical expressions:

- Be sure to use the correct field or combination of fields as intended by the analytic procedure dictated by the fraud committed.
- Ensure data integrity principles are applied at all times by following the system design and system rules.

- Use correct unique keys when relating tables
- Apply the correct order of operations when performing mathematical calculations, i.e. brackets first, powers and root before multiplication/ division followed by add/subtract
- Apply the correct order of programming operators; i.e. “NOT” first, followed by “AND” and lastly “OR”.
- When workings with date fields take note of the date format, e.g. “YYMMDD” versus “YYYYMMDD”, etc. Note that the software screen display may differ from the actual field layout.
- Ensure the correct syntax/ punctuation is used when referring to fields in technical expressions, e.g. when workings with text fields use the appropriate text qualifier such as double quotes.
- Always apply professional scepticism and double check your expression after executing. The software will execute a valid technical command with its parameters but cannot confirm whether the expression addresses the analytical procedure correctly. For example, the analytical procedure requires an extract of all transactions on Monday and Tuesday. The correct technical expression will be: Day = “Monday” OR Day = “Tuesday” and NOT Day = “Monday” AND Day = “Tuesday”. Both will yield results but the latter will be incorrect. In actual fact the second result is zero as one field (Day) cannot have two values at the same time.

*NB! Rule of thumb - if the result is zero the technical expression is most likely incorrect.*

Review and Interpret the results

It is very important that the data analyst at all times evaluate the results before reaching any conclusions or distributing the results to the audit team or fraud investigator.

When reviewing the initial results apply the following:

- At first glance evaluate the reasonability of the result against your expected result. For instance, it is most unlikely that the result will yield 90% of the starting population transactions.
- Check the technical expression used to obtain the result for possible errors
- Visually confirm the result against the expression applied meaning if the technical expression was to exclude all transactions below the value of 1 000 it is not expected to see any values below 1 000 in the results file.
- The technical expression may be correct but the result is not focused enough. This may be due to having missed system parameters thus refine the test.
- Pattern recognition is very useful in fault finding. Patterns can assist in identifying unknown criteria to adjust the analytical procedure or point the investigation into another direction.
- Corroborate the analytic results with other sources such as physical invoices, cheques, etc. If not available apply reverse engineering on the results for assurance. For example, the data analyst may have stratified the total population into three distinct stratums thus the three stratums added together should be equal to the full population. Discrepancies may highlight technical expression errors.

# Section 2 - Proactive fraud analytics

Scope of proactive fraud analytics

Proactive fraud analytics will assist the auditor to address the intended objectives of ISA240 which are:

- To identify and assess the risks of material misstatement of the financial statements due to fraud;
- To obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatement due to fraud, through designing and implementing appropriate responses; and
- To respond appropriately to fraud or suspected fraud identified during the audit.

Though the objectives seems to limit the fraud assessment to only **financial statement fraud** ISA240 in paragraph 11 extends the meaning by defining ***fraud*** and ***fraud risk indicators*** as follows***:***

***Fraud*** – An intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage.

***Fraud risk factors*** – Events or conditions that indicate an incentive or pressure to commit fraud or provide an opportunity to commit fraud.

The definition of ***Fraud*** by ISA240 lends itself to the ACFE classification of occupational fraud as set out above in section 1 which is:

- Asset misappropriation
- Financial statement fraud; and
- Corruption

The proactive fraud analytics aims to satisfy the auditor's assessment of ***Fraud risk factors*** through performing data analytics and applying the outcomes of the data analytics into a fraud risk scoring model.

Before the fraud scoring model can be discussed it is necessary to introduce the analytical fraud scheme assessment tool.

## ANALYTICAL FRAUD SCHEME ASSESSMENT TOOL

The analytical fraud scheme assessment tool enables the auditor to make use of data analytics to assess the presence of possible fraud. *The presence of the possibility of fraud will be concluded upon if documented fraud indicator(s) are occurring in transactional data uncovered/ confirmed by purposeful designed data analytical procedures.*

The elements of the analytical tool and graphically represented below are:

- Fraud characteristic
- Fraud indicator
- Analytical procedure
- Importance
- Control failure
- Data requirement

| FRAUD SCHEME | | | | | |
|---|---|---|---|---|---|
| **Characteristic** | **Fraud Indicator** | **Analytical procedure** | **Importance** | **Control Failure** | **Info/ data needed** |
| Characterisitc 1 | Indicator 1 | Analytic 1 | 1 | | Fields required to execute analytic procedure |
| | | Analytic 2 | 2 | Yes | |
| | | Analytic 3 | 1 | | |
| | Indicator 2 | Analytic 4 | 2 | Yes | |
| | | Analytic 5 | 1 | | |
| | | Analytic 6 | 1 | | |
| | | Analytic 7 | 1 | | |
| | | Analytic 8 | 1 | | |
| | | Analytic 9 | 1 | | |
| | | Analytic 10 | 1 | | |
| | | Analytic 11 | 1 | | |
| Characteristic 2 | Indicator 3 | Analytic 12 | 1 | | |
| | | Analytic 13 | 2 | Yes | |
| | | Analytic 14 | 1 | | |
| Characteristic 3 | Indicator 4 | Analytic 15 | 1 | | |
| | | Analytic 16 | 1 | Yes | |
| | | Analytic 17 | 1 | | |
| | | Analytic 18 | 1 | | |

To perform a data analytical approach to fraud assessment the fraud scheme has to be researched, fully documented and mapped to analytical procedures. The tool has further to provide for evaluation criteria that will inform the fraud scoring model in the end. The workings and evaluation of the fraud assessment tool is elaborated upon and described below followed by a practical example in as per the template above.

Each fraud scheme needs to be separately documented in the above template.

Fraud characteristic

In assessing the fraud scheme each scheme is analysed to determine the characteristics of the scheme meaning how the scheme works (modus operandi) and the fraud is perpetrated. Each fraud scheme may have more than one characteristic.

Fraud indicator

Each fraud characteristic has specific fraud drivers (actions) that when successfully applied makes the fraud possible. The fraud driver is then captured as a fraud indicator representing the fraud scheme. Each characteristic may have more than one fraud indicator

Analytical procedure

Each fraud indicator is then assessed in terms of data behaviour meaning that the fraud indicator has a distinct footprint represented by data. The footprint is documented as an analytical procedure relating to the fraud indicator. A fraud indicator may have more than one associated analytical procedure. This is the core of the fraud assessment tool. The presence of a fraud characteristic or indicator depend solely whether the analytical procedure returns a positive answer, i.e. whether the footprint exists or not (confirmation).

Importance rating

Each analytical procedure is independently assessed for importance. It is accepted that the prevalence of certain analytical procedures of a specific fraud indicator is more likely to represent the fraud scheme than another which is then assigned higher importance value of 2. All other analytical procedures are assigned a value of 1. The importance values will be used during in the fraud scoring model.

Control failure

The majority of fraud occurs as a result of a specific weakness being present that can be exploited and more so the culprit lies at internal control failures. Each analytical procedure may also reflect whether it results from a possible control failure. Should a specific analytical procedure be confirmed and there is an associated/ perceived control failure it will inform the fraud scoring model. See fraud scoring model below on *hardening factors*.

Info/ data needed

The template lists all the required fields that are needed to perform the analytical procedure as well as the system/ table the field is typically sourced from.

Example of a completed fraud scheme assessment

| False invoicing: Pass through | | | | | |
|---|---|---|---|---|---|
| **Characteristic** | **Fraud Indicator** | **Analytical procedure** | **Importance** | **Control Failure** | **Info/ data needed** |
| Shell company of employee/ employee associate used as middleman in providing goods and services | Goods and services are procured at higher than market prices | Determine the frequency of orders per supplier and identify suppliers that are diverging in excess to the norm | 1 | | Purchase ordering/ procurment system; fields of:<br>- buyer<br>- supplier<br>- date<br>- type of stock<br>- item number<br>- quantity<br>- amount<br>- price per unit (optional) |
| | | Determine whether a certain buyer has preferences when ordering items from a particular supplier | 2 | Yes | |
| | | Determine the costing/pricing of similar items per supplier and identify items diverging in excess to the norm | 1 | | |

Documented fraud scheme assessments for known frauds can be referred to in the Annexure under the three main areas of fraud as discussed in section1 namely asset misappropriation, financial statement fraud and corruption.

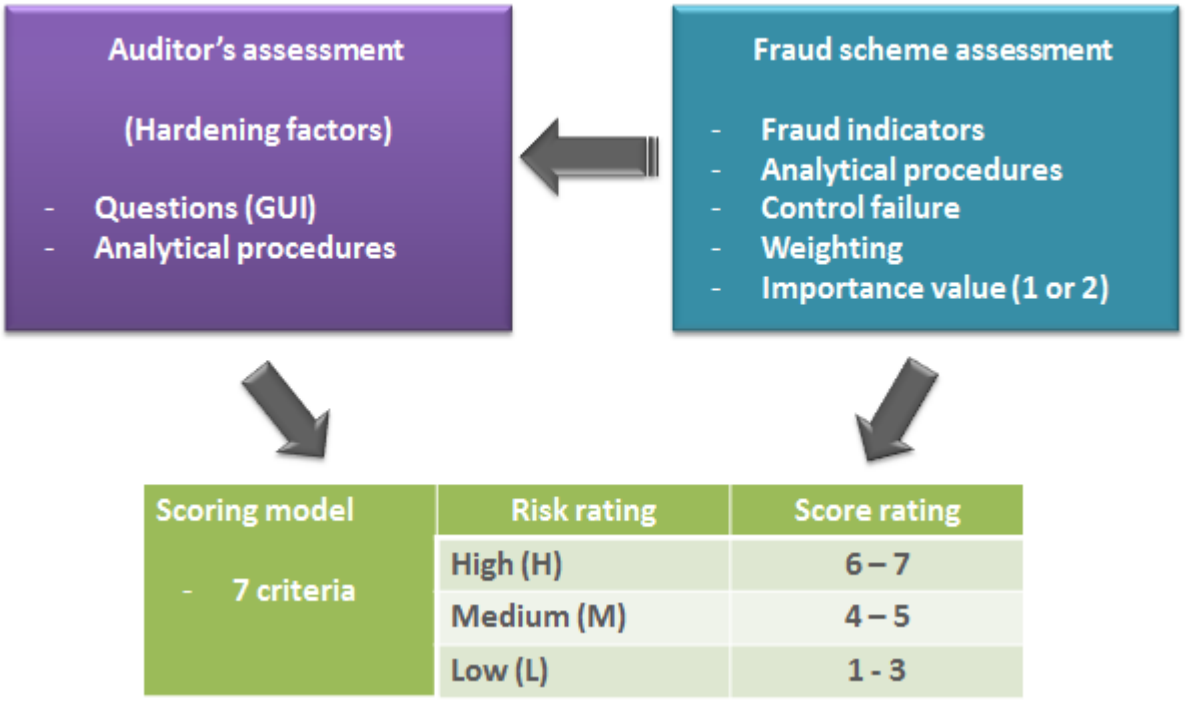
## FRAUD SCORING MODEL

The ACFE defines fraud scoring as a method of consolidating and aggregating results of tests that identify relationships and/or transactions that exhibit characteristics indicative of relatively high fraud risk.

A fraud scoring model is not absolute in its design but assists the auditor to assess the possibility of or likelihood of fraudulent misstatement occurring. The fraud scoring model's aim is usually to raise the alertness of the auditor to the possible occurrence (likelihood) of fraud and will either direct the auditor to areas of particular audit focus or confirm the auditor's professional scepticism surrounding the occurrence or non-occurrence of fraud.

The saying goes that where there is smoke there is a fire but finding one fraud indicator; a coincidence indicator does not constitute fraud nor warrant an excessive investigation. Fraud scoring will prevent misinterpretation by applying a risk-weighting matrix to fraud indicators, adjusted with scope to finally highlight the possibility of fraud. Fraud scoring is an art of science and a tool which reduces the need for guessing by the auditor and prevents wild goose chases.

The fraud scoring model is graphically represented below.




The fraud scoring starts with an auditor's assessment of the environment in terms of the ISA240 requirements and fraud scheme specific opinion. The auditor's assessment serves as "*hardening factors*" which is then aggregated with the analytical fraud scheme assessments to inform the overall scoring. "*Hardening factors*" provides the scoring model with higher likelihood of occurrence of fraud which then informs the analytical fraud scheme. Overlaps between the auditor's assessment and the analytical fraud scheme assessment then increases (compounds) the overall fraud rating.

The principles of the fraud scoring model are as follow:

- The model would provide a risk rating for each fraud scheme of **Low**, **Medium** or **High** indicating the anticipated level of exposure to fraud based on analysis.
- Scoring will be provided on the three areas of fraud; Asset misappropriation, financial statement fraud or corruption/ Bribery.
- The risk rating is attained from an aggregated score ranging from 1 to 7 which is categorised as being **Low** (Score of 1 to 3**), Medium** (score of 4 and 5) and **High** (score of 6 and 7).
- The scoring is derived from the number of positive outcomes against seven fraud assessment criteria (FSC) which are:
  - Is there an opportunity to commit fraud?
  - Does the scheme have a hardening factor present?
  - Scheme confirmation through analysis (weighted above 50%)
  - Were all core scheme analytics (important) confirmed?
  - Do the identified/impacted transactions represent a significant value (20%) of the entire population?
  - Have the majority (75% and above) of fraud indicators been confirmed by analysis?

- Do the identified/impacted transactions represent a significant value (20%) for the core indicators?

*Note: Each criteria carries equal weight of one*.

The meaning of each of the criteria (FSC) is explained below.

<u>FSC1: Is there an opportunity to commit fraud?</u>

The drivers/ motives to commit fraud have been widely published under the auspices of the *fraud triangle* (Cressey) or more currently the *fraud diamond* (Wolf and Hemanson – 2004). The fraud diamond uses the same three motives as the fraud triangle which is:

- Opportunity to commit fraud
  There is a weakness in the system which can be exploited.

- Pressure/ incentive to commit fraud
  There is a specific need to commit the fraud; e.g. in the case of AFS, to have the financial position appear better than it is.

- Rationalisation in committing the fraud
  Fraudster has the personal conviction that committing the fraud is the right thing to do under the circumstances.

The fraud diamond adds to the above the fourth motive which is the *capability* to commit fraud whereby the fraudster has position and authority to commit the fraud.

In determining the opportunity the auditor will provide his/her opinion based on questions. The questions focus on three of the motives above excluding *rationalisation* as this cannot be analytically assessed. The questions thus aim at assessing:

- Whether there is persons acting in key positions?
- Are there any vacancies in key positions?
- Are appropriate SODs in place?
- Is there a perceived/ expectation of control failures?
- Assessment of fraud management by management in terms of SA240 (par. 17 – 24).

Any of the questions which are supported by appropriate data can be analytically confirmed/ assessed as well outside of the auditor's assessment, e.g. SOD analysis.

This scoring criterion is assigned a positive outcome (1 point) should the any of the auditor assessment questions be positive (yes).

FSC2:Does the scheme have a hardening factor present?

Each fraud scheme has an auditor's assessment focusing on potential exposures from fraud. This is a questionnaire based assessment on the auditor's view of fraud exposure provided previous year's engagement and current year environmental assessment.
As this is a risk assessment the questionnaire provides for auditor judgmental considerations that may have an impact on the overall environment. These considerations are split into the main categories of occupational fraud defined in section 1 and expanded on with ISA240 considerations.

This scoring criterion is assigned a positive outcome (1 point) should the any of the auditor assessment questions be positive (yes). Nevertheless, it must be noted that these factors may be analytically assessed as well. For instance, control failure is listed as a factor but the auditor assessment was negative thus the scoring model would not assign any value. However, should an analytical procedure confirm a control failure this scoring criterion would be modified to assign a value (1 point) into the scoring model.

The detail of the auditor's assessment is set out in the Annexures.

FSC3: Scheme confirmation through analysis (weighted above 50%)

Each analytical procedure is assigned an importance value of either one (1) or two (2) thus an entire scheme would have a maximum value (scheme total) for importance by adding together all the assigned importance values.

Every analytical procedure would either be confirmed or not through data analysis. A positive score (1 point) is assigned for this scoring criterion if it is found that when totalling the importance values of confirmed analytics exceeds 50% of the scheme total.

FSC4: Were all core scheme analytics (important) confirmed?

A positive score (1 point) is assigned for this scoring criterion if all the core analytics of the fraud scheme was analytically confirmed. Core analytics is indicated by an importance value of 2 thus for a particular fraud scheme each (all) analytical procedure being deemed as highly representative of the fraud scheme or a fraud indicator has to be present.

FSC5: Do the identified/impacted transactions represent a significant value of the entire population?

Each analytical procedure focuses on a specific set of transactions and its associated value. In determining the outcome of this criterion a positive outcome (1 point) is assigned when it is found that the representative amount of all confirmed analytics for a particular fraud scheme is 20% or more of the total value of the fraud scheme. The formula is shown below.

$$\frac{Total\ of\ confirmed\ analytics\ values}{Total\ scheme\ value} >= 20\%$$

***Total of confirmed analytics values***: add together for the fraud scheme the value of transactions for confirmed analytics

***Total scheme value***: add together the value of all transactions of all the fraud scheme analytics

FSC6: Have the majority (above 75%) of fraud indicators been confirmed by analysis?

A fraud indicator is accepted as being confirmed when all the associated analytical procedures of the fraud indicator are confirmed. By example if a fraud indicator has three (3) associated analytical procedures all three have to be confirmed.

If one of the analytical procedures is a core analytic (importance = 2) which is confirmed but any of the other two was not confirmed the fraud indicator is not confirmed.

A positive score (1 point) is assigned when 75% or above of the fraud scheme's fraud indicators are confirmed.

FSC7: Do the identified/impacted transactions represent a significant value (20%) for the core indicators?

Each analytical procedure focuses on a specific set of transactions and its associated value. In determining the outcome of this criterion a positive outcome (1 point) is assigned when it is found that the representative amount of all confirmed core analytics (importance = 2) for a particular fraud indicator is 20% or more of the total value of the fraud indicator. The formula is shown below.

$$\frac{Total\ of\ confirmed\ core\ analytics\ values\ per fraud\ indicator}{Total\ Fraud\ indicator\ value} >= 20\%$$

***Total of confirmed core analytics values per fraud indicator***: add together for the fraud indicator the value of transactions for confirmed core analytics (importance value = 2) for a fraud indicator

***Total fraud indicator value***: add together the value of all transactions of all the fraud indicator analytical procedures.

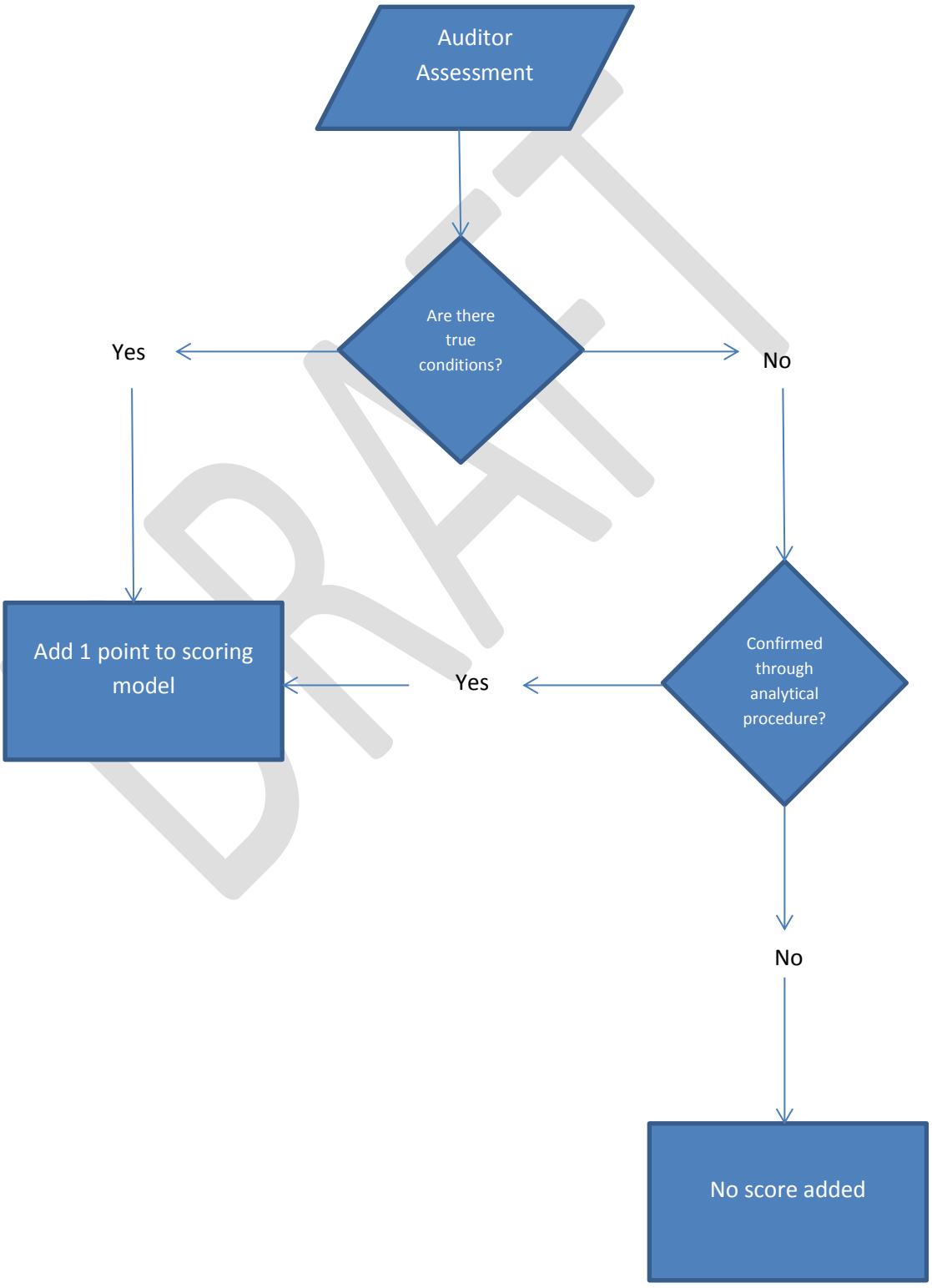
# Section 3

Building a pro-active analytics platform based on the adopted methodology (scoring model)

**DECISION TREE: scoring model**

Is there an opportunity to commit fraud?

Does the scheme have a hardening factor present?



**DECISION TREE: scoring model**

Scheme confirmation through analysis (weighted above 50%)

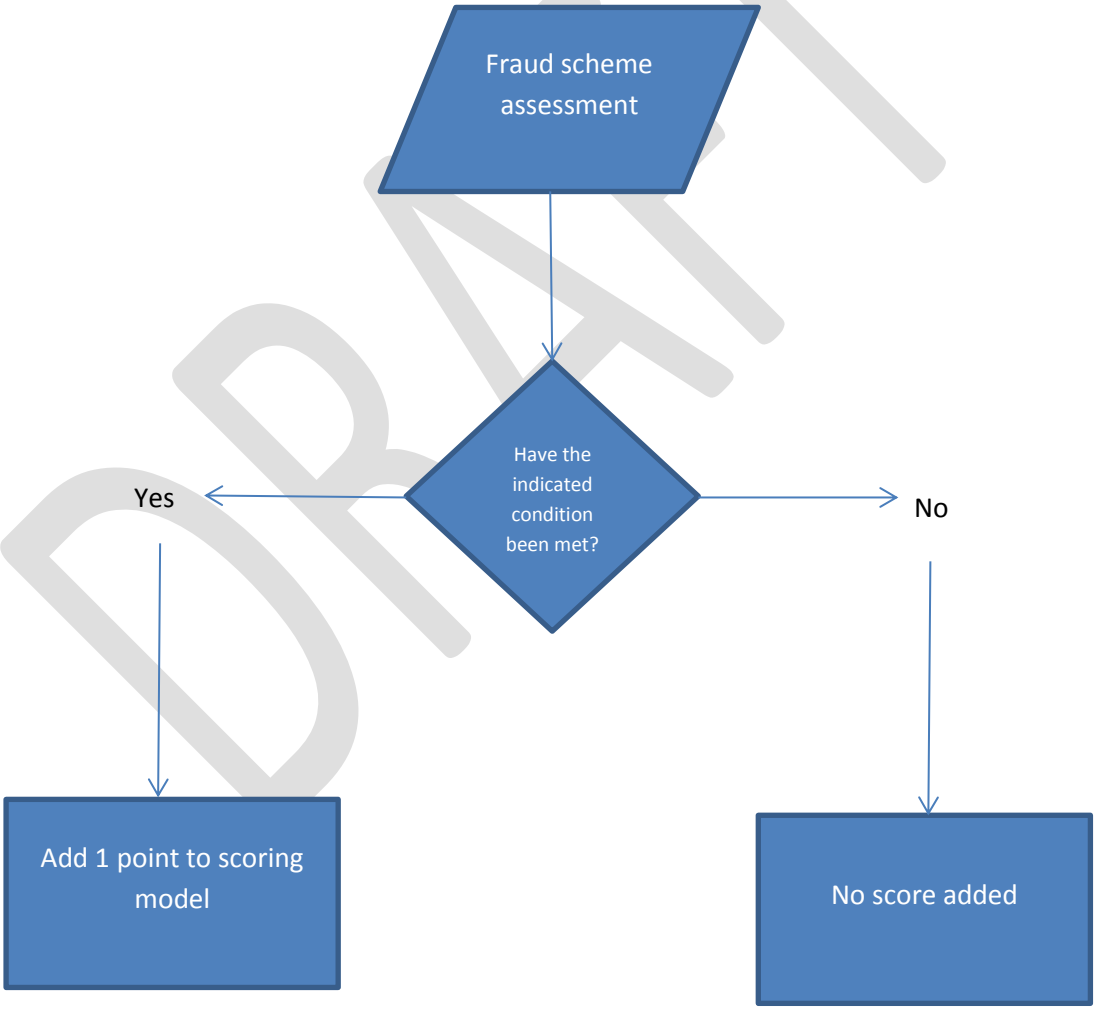
Were all core scheme analytics (important) confirmed?

Do the identified/impacted transactions represent a significant value of the entire population?

Have the majority (above 75%) of fraud indicators been confirmed by analysis?

Do the identified/impacted transactions represent a significant value (20%) for the core indicators?





## ANALYTICAL PROCEDURE MAPPING/MATRIX

| Program | SCHEME | INDICATOR | Analytical procedure | Importance | FSC1 | FSC2 (YC) | FSC3T | FSC3D (YC) | FSC4 (YC) | FSC5T | FSC5D (YC) | FSC6T | FSC6D (YC) | FSC7T | FSC7D (YC) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FAST | BS | ID1 | Analytic1 | 1 | | | T3 | D3 | | T5 | D5 | LT3 | LD3 | T71 | D71 |
| FAST | BS | ID1 | Analytic2 | 2 | | AM5 | T3 | D3 | L2 | T5 | D5 | LT3 | LD3 | T71 | D71 |
| FAST | BS | ID1 | Analytic3 | 1 | | | T3 | D3 | | T5 | D5 | LT3 | LD3 | T71 | D71 |
| FAST | BS | ID2 | Analytic4 | 2 | | AM5 | T3 | D3 | L2 | T5 | D5 | LT4 | LD4 | T72 | D72 |
| FAST | BS | ID2 | Analytic5 | 1 | | | T3 | D3 | | T5 | D5 | LT4 | LD4 | T72 | D72 |
| FAST | BS | ID2 | Analytic6 | 1 | | | T3 | D3 | | T5 | D5 | LT4 | LD4 | T72 | D72 |
| FAST | BS | ID2 | Analytic7 | 1 | | | T3 | D3 | | T5 | D5 | LT4 | LD4 | T72 | D72 |
| FAST | BS | ID2 | Analytic8 | 1 | | | T3 | D3 | | T5 | D5 | LT4 | LD4 | T72 | D72 |
| FAST | BS | ID2 | Analytic9 | 1 | | | T3 | D3 | | T5 | D5 | LT4 | LD4 | T72 | D72 |
| FAST | BS | ID2 | Analytic10 | 1 | | | T3 | D3 | | T5 | D5 | LT4 | LD4 | T72 | D72 |
| FAST | BS | ID2 | Analytic11 | 1 | | | T3 | D3 | | T5 | D5 | LT4 | LD4 | T72 | D72 |
| FAST | BS | ID3 | Analytic12 | 1 | | | T3 | D3 | | T5 | D5 | LT5 | LD5 | T73 | D73 |
| FAST | BS | ID3 | Analytic13 | 2 | | AM5 | T3 | D3 | L2 | T5 | D5 | LT5 | LD5 | T73 | D73 |
| FAST | BS | ID3 | Analytic14 | 1 | | | T3 | D3 | | T5 | D5 | LT5 | LD5 | T73 | D73 |
| FAST | BS | ID4 | Analytic15 | 1 | | | T3 | D3 | | T5 | D5 | LT6 | LD6 | T74 | D73 |
| FAST | BS | ID4 | Analytic16 | 1 | | AM5 | T3 | D3 | L2 | T5 | D5 | LT6 | LD6 | T74 | D73 |
| FAST | BS | ID4 | Analytic17 | 1 | | | T3 | D3 | | T5 | D5 | LT6 | LD6 | T74 | D73 |
| FAST | BS | ID4 | Analytic18 | 1 | | | T3 | D3 | | T5 | D5 | LT6 | LD6 | T74 | D73 |

Legend:
FAST = Fraud assessment tool
BS = Billing scheme
ID -= Fraud indicator
Y = Yes
YC = Yes if confirmed
FSC = Financial scoring criterion + (T) total + (D) detail
AM = Asset management
L = Logical

# ANNEXURES

# Annexure: Auditor's assessment (Hardening factors)

**International Standard on Auditing (ISA240) -**

| Auditor considerations on fraud management: | | Yes | No | High | Medium | Low |
|---|---|---|---|---|---|---|
| 1 | Is there a management (not IA) implemented fraud risk identification process in place? | | | | | |
| 2 | If yes in 1, what is management's assessment of fraud risk? | | | | | |
| 3 | Is there an ethical programme implemented? | | | | | |
| 4 | Is there an internal audit function? | | | | | |
| 5 | Is the governance structure independent from the management process of establishing and monitoring internal controls? | | | | | |

**Annual Financial Statement fraud**

| Auditor considerations on financial statements: | | Yes | No |
|---|---|---|---|
| 1 | Have risks been identified of material misstatement due to fraud? | | |
| 2 | If yes in 1, what area? | | |
| | > Revenue | | |
| | > Procurement | | |
| | > Payroll | | |
| | > Assets | | |
| 3 | Are there instances of SOD failures allowing management to override controls? | | |
| 4 | Are there incentives/ motives to alter AFS? | | |
| 5 | If yes 4, what area? | | |
| | > Performance | | |
| | > Profit/ going concern | | |
| | > Audit outcome | | |
| 6 | Are there confirmed instance(s) of fraud? | | |

**Asset Misappropriation (AM)**

| Auditor considerations on asset management | | Yes | No |
|---|---|---|---|
| 1 | Are any of the key positions in the supply chain management process: | | |
| | > Vacant? | | |
| | > Filled with acting capacity? | | |
| 2 | If "yes" in 1 for vacant, have the vacancy responsibilities been: | | |
| | > Allocated a single peer/ supervisor of the position? | | |
| | > Distributed between peers? | | |
| | > Allocated/ distributed to lower levels? | | |
| 3 | If "yes" in 1 for acting position, have the authorisations of the acting person for his/her normal duties been removed? | | |
| 4 | Are the principles of basic segregation between preparer and approver being followed? | | |
| 5 | Have any control failures been identified during the walkthrough? | | |
| | > Preparation | | |
| | > Approval | | |
| | > Reconciliation | | |
| 6 | Are there confirmed instance(s) of fraud? | | |

**Corruption/ Bribery**

| Auditor considerations on corruption: | | Yes | No |
|---|---|---|---|
| | | | |
| | | | |
| | **Still to be completed/ determined** | | |
| | | | |
| | | | |

# Annexure: Known fraud schemes

**Billing fraud schemes (BS)**

| Characteristic | Fraud indicator | Analytical Procedure | Importance | Control Failure | Info/ data needed |
|---|---|---|---|---|---|
| Shell company of employee/ employee associate used as middleman in providing goods and services | Goods and services are procured at higher than market prices (pass through scheme) | Determine the frequency of orders per supplier and identify suppliers that are diverging in excess to the norm | 1 | | Purchase ordering/ procurement system; fields of:<br>- buyer<br>- supplier<br>- date<br>- type of stock<br>- item number<br>- quantity<br>- amount<br>- price per unit (optional) |
| | | Determine whether a certain buyer has preferences when ordering items from a particular supplier | 2 | Yes | |
| | | Determine the costing/pricing of similar items per supplier and identify items diverging in excess to the norm | 1 | | |
| | Fictitious procurement of goods or services (false invoicing scheme) | Identify goods paid for but not taken up into inventory/ no GRN | 2 | Yes | |
| | | Identify goods paid for, taken up into inventory but inventory is cancelled/ adjusted | 1 | | |
| | | Identify partial deliveries off goods which is | 1 | | |

| Characteristic | Fraud indicator | Analytical Procedure | Importance | Control Failure | Info/ data needed |
|---|---|---|---|---|---|
| | | long outstanding and paid in full | | | |
| | | Identify invoices from the same company where there is little or no sequence between invoice numbers | 1 | | |
| | | Identify vendors that never makes use of a purchase order | 1 | | |
| | | Vendor details have similarity with employee details; e.g. address, bank account, telephone, company ownership | 1 | | |
| | | Vendors with that display data quality inconsistencies, e.g. no contact information or tax numbers | 1 | | |
| | | Vendors have different delivery address from their street and/or billing address | 1 | | |
| Pay and return scheme | Mishandling of legitimate vendor payments | Increased activity on vendors that had minimal purchases in prior periods yet having unusual high | 1 | | |

| Characteristic | Fraud indicator | Analytical Procedure | Importance | Control Failure | Info/ data needed |
|---|---|---|---|---|---|
| | | activity payments in current periods or suspended vendors re-activated with high usage | | | |
| | | Identification of duplicate payments based on the vendor, invoice number, amount | 2 | Yes | |
| | | Identify significant increases in the average price per item | 1 | | |
| General billing fraud | General indicators for billing | Prevalence of rounded numbers payments | 1 | | |
| | | Extract all payments with no related invoice | 1 | Yes | |
| | | Vendors paid (EFT) are not on the vendor master file | 1 | | |
| | | Frequent changes to vendor Masterfile; bank account changes | 1 | | |