FRAUD IS NOT COMPLICATED – A pro-active fraud audit approach

What is fraud?

Fraud is the abuse of trust and the exploitation of basic checks and balances which we often neglect in doing right consistently. And it happens because we do not have a proper understanding of our systems, our processes, the data generated by these and our staff. It is that simple! Be honest with yourself and look at every matter ever investigated by your team or company. How complicated was the actual fraud or modus operandi. In more than 90% of the cases it is rarely something where you require a specialist with PHD level qualifications and I have successfully investigated my share of chartered accountants, doctors, engineers and actuaries.

Decreased effectiveness of internal audit functions

Recent surveys such as KPMG's "Profile of a fraudster" and PwC's "Global economic crime survey" state clearly that the effectiveness of internal audit functions to detect and prevent fraud are decreasing.

Why? The reasons are numerous such as the lack of proper capacitation of these functions (an excuse which is always thrown into the mix) and the recent "key-controls-focus" approach which are becoming the norm unfortunately (the latter reason is my own conclusion). However, one of the many reasons which stand out for me is the lack of quality exposure to actual fraudulent matters and ineffective collaborations between this unit and the investigators. Internal audit does not understand fraud and they try and throw complicated methodologies at the problem. You must fight fire with fire – build trust and understand your business.

The most successful fraudsters are those who came through the ranks, i.e. those individuals who have an intimate knowledge of the "back office" and sub-processes. All businesses (at their core) have the same systems and processes to manage their income, assets, creditors, and funds. What makes your business unique (when compared to any other business) is your staff, the mix of cultures and the different management styles. Fraudsters are way ahead in this – they know when and how to push our buttons.

The "Loose-thread-theory"

With a "key-controls-focus" you are missing stuff. There is something we call the "Loose-thread-theory" which basically says that when applying significance and likelihood type approaches in ranking and addressing potential risks you are leaving a multitude of "loose threads" in your wake. These "loose threads", when activated in combination or simultaneously, could still allow significant frauds to happen undetected. Therefore, if only the significant threads are sorted, the smaller ones could still leave you with no jersey (I know it is a poor attempt at imagery but you get the idea).

The fraud triangle revisited

The fraud triangle has been around for a while, but do we truly understand its implications and relevance in the fight against fraud and corruption? We spent too much time and money on only one leg of the triangle, i.e. opportunity. That is why fortunes are being spent on external and internal audits,

building investigative capacities, investing in data mining tools, investing in the latest preventative technologies, etc.

We ignore for instance the human side of the triangle, i.e. rationalisation and pressures experienced by potential fraudsters and your staff. This is where building trust, demonstrating your objectivity and demonstrating your persistence in assisting staff and whistle blowers can have a major impact without breaking the bank.

Picking up the slack

The work of investigation units in an organisation is increasing because they are picking up the pieces left behind by the ineffectiveness of internal audit units. This is not a lambasting of internal audit, but rather a wake-up call that there is a real divide between the efforts of these two units and to address this both units first have to acknowledge each other for the sets of skills each unit is bringing to the table and that better collaboration is required.

For this to work true independence of each unit is required, i.e. the investigative unit should not report to the internal audit unit. But alas they often view the investigators as a bunch of cops/"cowboys" who must be policed, controlled and kept in a rigid structure according to internal audit norms. This is not effective!

Internal audit's skill shortage sorted

The special investigative units or forensic services functions in your organization is well qualified and much better positioned to complement the function and effectiveness of internal audit. The best internal auditor is someone who has spent sufficient time as an investigator – I have seen this in practice and it works well. Why? Because investigators have lost their blinkers long ago – probably with their very first investigation. Investigative units spend more time on the ground with all levels of staff.

Traditional internal audit training cannot equip an internal auditor with the wealth of experience obtained when conducting investigations. Maybe their training should make it compulsory to first spend at least 12 months (as part of articles or something similar) in an investigative unit doing actual investigations before they try their hand at internal auditing. Just a thought – use it or lose it!

Thus, when looking at improving the effectiveness of your processes in detecting and preventing fraud, the skills and experience of your investigative units must be pulled together and refocused to move from a merely reactive approach to a truly pro-active approach.

What is required?

One way of addressing the issues briefly touched on above is a pro-active fraud audit or review (or "fraudit"). When conducted properly, it will have a major impact in your fight against fraud and corruption. The registered auditors must excuse me for using their term "audit" so freely, but at least everyone understand what it means and what it entails. Some of you may have attempted this type of review/audit in the past with varying degrees of success. In this document I will attempt to explain my approach and the various essential inputs required to do this effectively.

A fraud investigator and the accompanying fraud risk management process can change an organization – it can impact on moral in a positive way. Most employees are there to actually work and earn a salary, but if you treat them like crap they will turn on you.

What is a pro-active fraud audit (or "fraudit")?

Let us first start with a definition. What is a pro-active fraud audit? It is an in-depth review of a process where you combine the skills of an experienced fraud investigator and internal auditor to conduct a detail walk through of a process. Evident here is the required collaboration between the two units or find someone with both skill sets (call me for some references).

You will be required to conduct the following as part of this process:

- Background checks on every individual (or at least key individuals) in the process. This does not refer to only a CIPRO (company/director search) or Transunion/ITC/Experian/credit check, but also the use of Google to search the internet for an individual's (including, as per their personnel files, their next of kin's) name, telephone numbers and addresses. You could identify other businesses operated by these individuals and these could be listed as suppliers on your systems. On Google StreetView[1] you will note whether his/her house stands out from the neighbouring houses, i.e. whether more money was spent on renovations than what is generally available in the area where he/she stays;
- Similar background checks on any entity (customer or supplier) relevant to the process;
- Data mining for interesting trends. Trends which may indicate fraud, but also (more importantly) trends which help you to better understand the process flow of information and the activities of staff;
- Results of previous allegations, internal audits and investigations;
- Breaking a process up into its sub-components and individual actions;
- Critical analysis of supporting documentation and explanations provided;
- Critical impact analysis[2] of a process and its sub-components/actions; and
- Critical impact analysis[3] of each individual's actions in the process in order to establish the role they play in the process and the impact their work has on other individuals in the process.

[1] StreetView provides a snapshot of a neighbourhood at a certain point in time. Sometimes you can even consider driving past an employee's house to see how many changes were made since the StreetView images.
[2] These impact analyses are key in this approach, but you require a sound and practical understanding of basic audit concepts such as those listed on page 6 of this document.
[3] Refer footnote 2 above.

Fraudit – A quick how to?

Here I will attempt to provide a step-by-step approach at a high level:

Step 1 *– Where does the process end up in the reported numbers and bottom line?*

I usually start with the financial statements or most recent monthly management reports. Or rather, first decide which process or system you want to focus your efforts on and then go to the financials and/or monthly reports.

Now ask someone (finance manager, financial director, accountant, etc.) to explain how they arrived at the reported results from the totals generated by your core ERP/ERM (such as SAP or whatever systems your company utilise). A NOTE FOR THE YOUNG INITIATES: *The risk of fraud increases with the number of Excel spreadsheets required to explain the difference between the reported results and the core systems, i.e. the higher the number of spreadsheets the higher the risk of fraud. Make sure you get an electronic copy of these spreadsheets and review each formula and look for hidden cells, columns and rows. I have found "sum-formulas" containing "+R100 000", as well as hidden rows to conceal problem areas.*

During this step you should identify all systems and sub-processes which add to the totals reflected in the reported results.

War story #1: BOLT-ly going where so many was before and probably still is

My client is an insurance company with a billion plus turnover (in SA Rands please – don't get too excited). I attempted Step 1 in respect of the total claims paid for a particular financial year. Based on my discussions with the internal audit unit, I was informed that the entity operates its own in-house developed system for managing claims (from registration to final pay-out and summarising the claim, i.e. the complete claims process). However, when they started showing me the Excel spreadsheets required to compile the results from only "*one*" system (as I was led to believe by the internal auditors) it became clear that something was amiss. I requested explanations for some of the various totals contained in the spreadsheets which clearly did not come from the reports I obtained from the core claims system. The following explanations were provided for some of the totals:

1. **To the past we BOLT-ed**
   "*Ahhh yes those are from the BOLT system (not their core system). You see we bought this other company a few years ago and BOLT was their system…we are in the process of phasing it out, i.e. no new business is done on it. We are only finalising old claims pre-dating the date when we bought the company.*" I asked them what was the average time it took their staff to process a claim and the answer was less than a year. Thus, how can old claims still be active on a system bought several years ago??? They responded with: "*It is an old system and not much is going on there…just a few small payments now and then*". Well people, those few small payments added up to a multi-million Rand fraud perpetrated by two females in senior positions for at least the last 5 years. The one lady came from the old company and new the BOLT system well. My client allowed the system to be set up in such a way that whatever is processed on the BOLT system, is cleared on a weekly basis as one total to the main bank account of my client and for reporting purposes totals per claim type is generated by our two ladies…no further detail…no nothing further. They had complete autonomy and they lived the high life. Various payments were made to fictitious claimants and suppliers. The internal auditors and management never came close to this system as they saw it as an old/legacy system being phased out and not much is happening on it, i.e. the amounts are below "*materiality*" (although a strictly external audit term it became clear that they were thinking along the lines of "*whatever makes the external auditors happy*").

2. Salvage and third party recoveries are controlled by someone somewhere…we think…phone switchboard

"*Ohh…those totals are never of any noteworthy value. They come from the summaries provided by the third party recovery branch and those are from the salvage guys.*" Here we identified peripheral processes which did not operate via the core ERM/ERP system. Thus, these peripheral processes were manual processes performed by small groups of people autonomous from the core process. These groups also operated at separate offices a few kilometres away from the head offices. Thus, they were running their own little empire. Again multi-million rand frauds for an extended period. Insurance companies are losing millions annually on salvage and 3rd party related transactions. A few simple checks and controls can curtail this…but alas…as long as more premiums come in than claims paid they are happy.

***Step 2** – Identify the operational location for each sub-process and peripheral process*

Once you have identified all the sub-processes and peripheral processes of the core process for your *fraudit*, you will now be required to identify where each of these components are located, i.e. where are the offices/units/staff located for each. ANOTHER NOTE FOR THE YOUNG INITIATES: *The further an office/unit/staff of a component is from the head office or main office for that province/region, the higher the risk of fraud. Because: they have more autonomy and less physical management oversight of their daily activities.*

Also compile a list of staff members for each sub-process and location. You can start with some background checks on these individuals. Consider obtaining each individual's job description and their KPIs (i.e. key performance indicators) or performance metrics in order to obtain an understanding of what their basic duties are. Remember that some frauds are merely the manipulation of results to ensure that you meet your KPIs/performance metrics and thus ensuring your bonus gets paid. Furthermore, when getting to grips with what individuals are actually doing in a process, I have often noted that their actual duties and KPIs are not properly aligned or the KPIs lack sufficient detail. If you can ensure that a person's KPIs are reflecting their true role and involvement in a process they become more accountable for their actions and the risk of fraud decreases significantly. I have had numerous altercations (that's putting it lightly) with management and HR on these issues. But here you have to work with the staff…if you can demonstrate to them how properly developed KPIs (aligned with their properly developed job descriptions) can actually protect them when things go wrong you will get their buy-in very quickly.

***Step 3** – Obtain documented standard operating procedures, past internal audit reports, investigations and allegations pertaining to each*

This should provide you with background information regarding each area and the common problems experienced there (if any). This will also equip you with an understanding of any acronyms or process-specific-terminology. Thus, enabling you to talk with some level of authority about a process without sounding like a complete idiot.

***Step 4** – Obtain as much data as possible from the systems available to you regarding each sub-process and location*

This data must be analysed sufficiently in order to enable you to start asking relevant questions during the next step. Look at the active users according to the data. Who don't you see in the data? What level of segregation can you detect from the data?

Step 5 *– Visit and break it down*

Why was the previous steps required? It all stems from what we as fraud investigators do on a daily basis…we develop a picture of what lies ahead…you start formulating potential questions and scenarios? A senior advocate once taught me that the trick to a successful interrogation/interview is "*for every question you must be 90% sure of the answer you'll receive and for the other 10% you must have more questions ready*"...that requires **preparation**!

Now you get your hands dirty and visit each location and perform a detail walk-through and review of the processes. Understand how they initiate their work, what information/goods do they receive from where in order to conduct their work, what they do with that information and how/what do they report to the main office. Do they use their own suppliers? Don't forget the steps preceding this section (such as background checks and impact analyses).

During this part you must consider basic concepts such as:

- Segregation of duties
- Conflicts of interests
- Completeness
- Accuracy
- Validity

These concepts must be considered during every action identified and reviewed by you, i.e. every action of an individual has an effect or impact on the next action or individual. What is the next individual doing to ensure that what he received from the previous action is complete and accurate? Does an individual have control over the impact/results of his actions which addresses his KPIs? Does he have control over the outcome of the following actions in any way? Does he have any influence in the outcome of the next individual's actions and duties?

War story #2 – Training the trainee

A person was a new recruit responsible for checking supporting documents before loading it for payment. He was still in his compulsory 3 month probation/training period. Once these documents were loaded, Mrs T Rainer was required to authorise these payments for final payment. However, when I visited his desk I noted that he first piled all the "checked" documents to one side before he captures it. My first thought was that he was trying to be efficient by first compiling all the documents and then capturing them in bulk instead of after each set of individual payment documents. But, that was not the case. He explained that he is still in his probation/training period and that he is required to present the documents (which are ready for capturing) to Mrs T Rainer (his predecessor) for final review and comments before he is allowed to capture the documents. Thus, we have a segregation of duty issue which was not evident when I reviewed the standard operating procedures as prepared by the internal audit unit. And seeing that the latter conducted a "key-controls-approach" they had spent more time in the manager's office talking about things than actually getting to know the actual process. Mrs T Rainer

was caught guiding him past certain glaring discrepancies on invoices from suppliers where her family was employed.

The benefits of a "fraudit"

- It is a "rubber soled" approach to better understand your processes;
- Identification of control breakdowns or lack of controls which could lead to fraud and corruption (especially the indirect ones);
- Identification of significant mal-alignments between documented standard operating procedures and actual actions;
- Identification of actual fraud and corruption in the relevant process or system;
- Identification of real root causes which caused the breakdowns, lack of controls and actual instances of fraud and corruption;

War story #3 – Real root causes are often not contained in internal audit textbooks

My client has a big manufacturing concern and exports globally. They knew they had a syndicate operating in the manufacturing plant, but they could not pin-point who and how they are doing it. The internal auditors, when conducting their internal audit at the factory, divided the factory into 2 logical sections, i.e. the manufacturing component and the finished goods (including distribution) component. Thus, they assigned a team per section, but they never compared notes…just the issues. Without going into too much detail here is a summary of what happened: I requested the systems' description (or standard operating procedures) and with this in hand I walked through the process with the internal audit team. On the manufacturing side they referred to PC1 (i.e. production clerk number 1) who is responsible for compiling the results of the manufacturing process and capturing these into SAP. On the finished goods side they referred to PC2 (i.e. production clerk number 2) who was responsible for counting the final manufactured goods to be transferred to the finished goods warehouse. PC2 is then required to capture these quantities into SAP. However, when I requested to meet PC1 and PC2, they were one and the same person. She was a key "employee" of the syndicate as she was able to manipulate the manufacturing results and finished goods' transfers in order to ensure that the wastage calculations did not exceed management's expectations. The internal auditors were (for want of a better term) flabbergasted…speechless…responding with "*But we…uhhh..key controls…uhhh…different teams…our audit software does not provide for…etc etc etc*".

Furthermore, I always make sure that I talk to the fraudsters in order to get a better understanding of their motivations. One person who worked in the warehouse (he was responsible for allocating loads to the trucks and was also a key member of the syndicate) explained the following which was all confirmed by us at a later stage: He had to relocate from Limpopo to Gauteng in order to maintain his job. My client recently closed their smaller factories, such as the one in Limpopo. My client offered them retrenchment packages or relocation. He picked the relocation option. However, he was a single parent and he had no family structure in Gauteng to fall back on and to assist him. Therefore, his son had to get a taxi from school every afternoon and sit in his dad's car till he finishes work, which was often late at night due to export loads being readied for departure the next morning including weekends. There was also compulsory daily stock counts to be conducted as the stock was popular syndicate and smuggling targets. He then had to go home and do chores such as homework with his son and then the

cycle repeats itself the next day. He was stretched and tired. He saw the syndicate as an opportunity to save money and get him and his son out of that situation. I am not getting soft here, but imagine yourself in that situation…just for once be honest with yourself and try and place yourself in such a situation! What would you have done? You have no family or friends in the area, you are missing out on your child's childhood by burning the candles on both ends and other job opportunities are scarce. A lot of parents would have gone the way he did.

I presented these findings to my client and they immediately instructed their HR division to conduct a survey in order to establish the personal challenges of their staff. This resulted in the building of child care facilities close to the premises because they realised that a lot of their staff had similar issues. Morale increased dramatically. What is the lesson here? Some root causes are not in a textbook. These root causes can only be identified when you meet your staff and you get to know them…a "fraudit" accomplishes this!

- Recommendations regarding effective and practical measures to address the control gaps and "real" root causes identified because of our "rubber soles";
- Discussions with the internal auditors regarding possible amendments to their internal audit plan and approach;
- Recommendations to management/executive regarding possible actions to take when actual fraud and corruption is identified; and
- Increased accountability of management and staff regarding their areas of responsibility

Yes...initially it will take longer than the average internal audit of the same process, but with experience you will become more efficient.

BUT: It is in-depth and thorough.

It considers all possibilities.

No key-control-focus, rather all controls.

It looks at everyone and their individual roles in a process.

It breaks each process down into its sub-components/actions.

It evaluates these actions and the individuals in relation to each other and their impact on each other.

It is a "*rubber sole*" approach.

AND: You <u>meet</u> the people!

Fraud is in the detail – Fraud exploits the basics so often neglected by us.

Remember: **D**$_f$**E**$_r$**T**$_o$**A**$_u$**I**$_d$**L** (Maybe there is a reason why the word "fraud" fits so snuggly in the word "detail".)

This was high-level, but I hope it helped in some way. I will in future try to update and amend with further lessons learned in the past and in the future.

I remember the first time when I spent time with an internal audit unit while they were "auditing" a process. The one chap commented that I knew quite a lot about audit assertions and internal auditing for a "policeman". He was quite surprised to learn that I actually did my articles at PwC and that my background was actually accounting and auditing. It then became clear to me that in most organisations there is this divide between investigators and internal audit, where investigators are still being viewed as "police officials" with no clue about auditing. But we are much better equipped and positioned in the organisation to do this work by just applying what is second nature for us…question, analyse, verify and never assume!

War story #3 – A final one: Another root cause not in the text books (I call this "The revenge that back fired")

A female who worked in a logistics department of a manufacturing client of mine defrauded the company of approximately R8 million over a period of 2 years. I had a long and emotional chat with her...please note that she was the one crying and I was just listening. Why did she start with the scheme? What motivated her? A few months before her first fraudulent payment, her employer conducted a company-wide HIV awareness drive. This included voluntary testing by an independent clinic. Her results were accidentally switched with an employee in the factory and she was informed that she was HIV positive. This was a shock to her and she immediately, at her own expense, went for another test which indicated that she was in fact HIV negative. BUT, the story soon spread in her community. She was very active in the local church and served on almost all the committees of that church. But as so often happens and people are people, she was marginalised and frowned upon by her church and its members. She resigned from every committee and never went back to the church. Her life and standing in the community were in tatters. Never during any of this did her employer or the HR department come to her defence. They did not warn staff to stop spreading rumours and that there was an accidental switching of results. They never stood up for her and informed people that by spreading unfounded rumours they are guilty of defamation of character and could be sued and they will help her in that process. They never took any action against the independent clinic, because it was run by a wife of one of the directors! Her fraud was motivated by revenge. Thus, this fraud could have been prevented if the employer and the HR department actually stood up to defend her. They could have prevented a loss of R8 million. So who is to blame here? Makes you think!