



Editorial...

Welcome to the Spring 2010 issue!

This edition is a bumper issue - not much work was done between June and July this year due to the 2010 Soccer World cup hence we did not compile a mid-year issue - who would have read it!?

The first article discusses the [2010 Soccer World](#) cup that was successfully hosted in South Africa and goes on to list some business analogies that we derived from watching all these soccer matches.

The second article focuses on the fact that the word **'RISK' is no longer a 4-letter word** and it should be freely discussed within organisations before it does become a 4-letter word!

We then discuss the key findings from two 2010 reports:

The [2010 ACFE Report To The Nations](#). The 'S' is in capitals because this is the first time since the report's conception in 2002 that countries other than the USA are surveyed.

The other report is the COSO report on [Fraudulent Financial Reporting: 1998-2007](#). Please don't gloss over this one thinking that it's an American report and doesn't apply to Africa.

Yes, most of the high-profile financial statement fraud cases have been American ones such as Enron, Worldcom, Tyco, Adelphia, HealthSouth, Phar-Mor, ZZZZBest, Crazy Eddie etc. but South Africa has had its fair share in Masterbond, MacMed, Beige, Regal Treasury Bank, Saambou, New Republic Bank, Tigon, Fidentia, Leasurenet etc!

We then focus on [who you should be calling to do your fraud prevention work or investigations](#). You don't go to a doctor that has not studied do you? Then why hire a person that is not accredited by a reputable organisation such as the Association of Certified Fraud Examiners?

If a suspect [defragments his computer hard drive](#) - does this mean the end of your investigation or is he (or she) doing you a favor?

[How Hot is Your Hotline](#) - most organisations have a hotline but how many of them are working? On average, 20% of employees know of some unethical behavior in an organisation - are you getting this amount of reports? If not maybe it's time you relooked at your disclosure service!

[Isn't it time your auditor got a coach?](#) The internal audit function is critical - do you provide enough support to this function?

[What happens to all your waste paper?](#) Identity theft attacks both individuals as well as organisations and criminals, known as 'dumpster divers'. go through your trash looking for information that they can use to defraud you. This article discusses Cleardata's service of shredding your waste paper onsite, BEFORE it's removed from your premises.

Lastly we look at the importance of [fraud and ethics awareness training](#) with an upcoming 4-day fraud prevention course being run by the IIA South Africa during November.

Mario Fazekas, Editor

Email: Mario@exactech.co.za

Mobile: 083 611 0161

The 2010 Soccer World Cup is finally over!

I say that with sadness and happiness.

1. I am not a sports fan so during the buildup to the tournament I had zero excitement, but after the opening match my wife and I were glued to the TV day after day.

We saw thousands of vehicles with flags and mirror socks...



and even the Exactech building was adorned with flags...



One of our clients had an eye-catching display of Makarapas (miner's helmets decorated with each countries' icons)...



And when we did the various SAICA fraud prevention workshops the hotels had some novel ways of demonstrating their soccer fever (lift doors and urinal)...



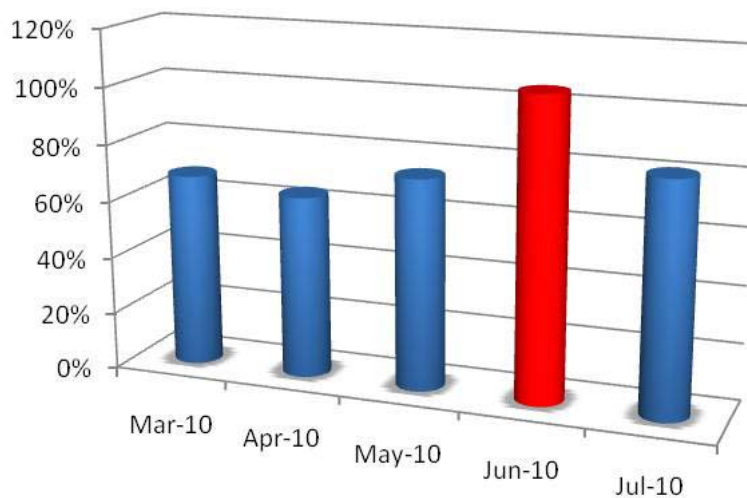
And now that the event is over we are having withdrawal symptoms! This is my sadness.

2. My happiness comes from the fact that after a month of doing nearly no business we can get back to business!

I thoroughly enjoyed the soccer and most matches provided us with lovely analogies that we see daily in our interactions with organisations and that we can now use to demonstrate why organisations seem to be losing the battle against fraud...

- Brazil came into the tournament with an arrogant attitude and as a result they went home with their tail between their legs. There are some arrogant companies out there who have a 'No Fraud Here' mentality - some of these companies don't exist anymore while others are simply playing Russian Roulette.
- Jay-Jay Okocher, the Nigerian soccer player and commentator said that African teams seem happy with just qualifying or making it to the round of 16 - they seemed to not have the determination or discipline to win. We often see this in organisations where discipline breaks down, controls are overridden & then fraud occurs. After the fraud there is discipline for just a few months until the novelty wears off & then we are back to the undisciplined way of doing business.
- There were quite a few selfish players or 'glory boys'. They wanted to score so that their names would go down in history as the hero - but they missed the goal but if they had of passed their teammate may have scored. One CFO said to me "I know we have a high fraud risk but I'm retiring in 18 months and I don't want to rock the boat!"
- Problems with the ball – in 2010 it's too round! In 2002 the Japanese ball was too light while in 2006 the German ball was too heavy. Making excuses instead of accepting our responsibilities to fight fraud and then taking action to ensure that our organisations have a best practice fraud prevention strategy in place and are therefore more profitable. The average organisation loses 5% of annual revenues to fraud each year - why are there still companies that are doing nothing to fight fraud?
- Technology lacking - Tennis and Cricket have been using technology for years with very good results but the stubbornness of the organizers kept this out of the Soccer World Cup - with unpleasant consequences! There are data analytic tools that would enable organisations to have a real-time feel of their business and detect frauds but so many companies are still not implementing CCM (Continuous Controls Monitoring).
- Portugal had the world's 'most expensive player', while Argentina had the world's 'best player'. The German team had the best team. Skill plus discipline. Individually, there were much better players in other teams but Germany were the most consistent team.
- The German team was not complacent – they would score a first goal then the second 'insurance goal and then two more! They kept up the standard and kept in control – things can go pear-shape very quickly if you drop your guard. Some companies get complacent and they stop monitoring controls or they start cutting spending on Internal Audit or fraud prevention and then they get defrauded.

- Germany used to be one of the top teams - they last won the world cup in 1990. Since then they have performed like a yo-yo. German soccer clubs then started a program in 1998 to train up the best players. This costs money but Germany in 2002 were runners up, in 2006 they came third and then in 2010 they came third again. It took over ten years and lots of money but they have reaped the rewards. How much are you spending on your fraud prevention programme?!
- Many people used the soccer world cup as an excuse to not do anything (they don't realise the criminals don't take time-off during sporting events, or over Christmas or other holidays!) The following graph shows that hotline calls of **Be Heard™** clients increased 30% during June 2010...



While the cat's away (at the matches) the rats come out to play!

- Some referees made very bad calls - the decisions that you as a CFO or other senior person make will have consequences. Don't spend money on fraud prevention and your organisation will give away about 5% of its turnover to the fraudsters. You will then be accountable to your board.
- Many hotels and lodges did not get the anticipated 'hordes of visitors' - because many of them had increased their prices by up to 100%! Tourists are not dumb and when they see this they make other plans. If your organisation gets greedy and doesn't want to spend money on fraud risk management the criminals, who are also not dumb, will see this and will exploit the weaknesses you are leaving open for them. ***'Penny-wise pound-foolish!'***
- If you want to gamble with your organisation's profits and your reputation you had better ask Paul the Octopus what your future holds before deciding to not implement a best-practice anti-fraud program. Besides Spain, he was the star of the show as he held the only 100% percent record of the tournament!
- It's not all doom and gloom - the rest of the world said that South Africa couldn't do it but we excelled! Tourists said this was their best world cup and they will be back to explore this beautiful country. Your organisation can reduce fraud and make itself a hard target - if you stick to best practice and implement all nine building blocks - so what are you waiting for...?

Where risk is no longer a four-letter word

Jonathan Le Roux , Member of Exactech Fraud Prevention Solutions

We all get into business for the same reasons, give or take a few.

It's about offering a service, offering a product, or both, that we firmly believe will make a difference to the people that we interact with. Many people, though, are equipped to be the expert in a business at one or two things – like delivery of the service, developing and selling the product, marketing the product, managing the office, and so on - but definitely not all...at least, not effectively.

If you are a SMME, you automatically get the 'master-of-all' job description as you don't have the luxury of employing more people to balance your risk-versus-reward appetite. If you are in a bigger organisation, you might have greater flexibility in having dedicated people who look after different aspects of your business risks, which allow you to focus on what you are good at.

Risk and Risk Management is not a term reserved for the C-Suite FTSE100 companies only! If you are in business – a one person show to 1000 person show, by default you are in and at risk, and you better have some tools in the Bob The Builder (Yes we Can!) toolbox of yours.

If you are a plumber, you are a Liquid (or not) Risk Manager. If you are a salesperson, you are a Content Risk Manager. If you are a restaurant owner, you are an Experience Risk Manager. If you are in financial services, you are a Wealth Creation Risk Manager.

Can you imagine boarding a plane and once you are in your seat, you hear an announcement that says the following:

"Good day ladies and gentleman. My name is Jonathan Le Roux and I am your Human Capital and Cargo Co-Coordivative Risk Manager.

My role here is to ensure that all the contents of this vessel (and the vessel itself) reach the end destination on your ticket safely and within the prescribed agreed to standard times. I will endeavour to get you there within a precision ratio of 98%.

I have a confidence level of 97% with a standard accepted deviation of 3% in achieving this objective. Do enjoy your flight, while our Food, Beverage and Interpersonal Risk Managers look after you."

We are all in risk or risk management. It just doesn't sound sexy, so we tend to play it down.

Risk is part of business and there are many tools and methodologies out there that can help businesses manage their risks effectively. But, you have first to determine how you can influence or manage the risk from a 'value creation' perspective, for example:

- Can you (your service/product) increase revenue?
- Can you (your service/product) increase profit margin?
- Can you (your service/product) 'sweat the assets' – increase efficiencies?
- Can you (your service/product) enhance company expectations to shareholders/investors?

If you (your product/service) create value and this value can contribute to an organisation's viability and sustainable growth, then RISK becomes no longer a four letter word. RISK now means:

- **Being Safe**
- **Being Sensible**
- **Being of Value**
- **Bringing focus on Return on Investment**
- **Bringing Governance to the fore**
- **Being mindful of one's environment and all that can influence it**

With this new found meaning of RISK, you start to realise the value of RISK and how inter-linked the risk/reward relationship actually is. Risk is not bad. Risk is, in fact, good. The viewing of risk with absolute disregard for people, planet or profit – this is bad.

Now RISK is the value creator and can be realised in assisting an organisation attain its objectives. So, you start to manage RISK with tools, spreadsheets, key risk indicators, monthly risk reports, and so on, and after 3-6 months of compiling these reports, getting the same information from the same people month on month, what do we notice?

Risk reports are the same – just tweak figures monthly (use standard 10% deviations!). Management just states: “Nothing changed since last month”.

You are spending more time on these reports for people who don't really read them (or take them or you seriously).

You are becoming bored with risk (and even believe people might be ganging up on you in the organisation as you are detracting them from business).

So then RISK becomes bad and we tend to stop looking at it and hope nothing bad happens – you know Murphy's Law, right?

Then, it happens, RISK becomes that other four letter word!

By then it is too little too late and we are on the back foot. We bring in external experts and re-engineer our entire processes, practically bringing business to a halt! This costs time, money and market share.

Then we stop and think.

***RISK is more than a four letter word, if we treat it right. So, from here on out: “Risk is my friend.”
Keep safe.***

jonathan@exactech.co.za

or

ask [Dr. J](#) on the [fit-FOR-fraud](#) Blog page

This article originally appeared in the August 2010 issue of COVER magazine.

Reprinted with permission from Cover Magazine - ***No hype, no speculation — just the facts***

The 2010 Report To The Nations on Occupational Fraud and Abuse

You don't want to start putting up Wanted posters in your offices, but the ACFE (Association of Certified Fraud Examiners) have published a very specific profile of the employee most likely to defraud your organisation.

Most company directors think their staff members are all honest but no one is above suspicion - fraudsters come in all shapes and sizes, from the most junior to most senior staff.

In the 2010 Report to the Nations, the ACFE have listed patterns on which staff members are more likely to defraud than others. In the past this study reflected only findings from US companies but this year it reflects a global picture and has 112 frauds from 21 African countries, of which 42% of the cases are from South Africa.

Based on their data here is the profile of the perpetrator of the most common frauds in African organisations:

Wanted –

- Male (75%)
- Aged 31-45 (56%)
- College or post graduate degree (52%)
- With the company more than 5 years (92%)
- Works in Accounting/Finance (40%)
- Managers and employees (88% [44% each])

Even though the managers and employees are equal in the number of fraud cases the managers steal more than double what the employees steal - an average of \$270 000 (R1.9 million) compared to the \$150 000 (R1 million) of the average employee fraudster.

So, you have a finance manager who is 43 and he has a post-graduate degree and has been with the organisation for 18 years - does that mean he's a fraudster?

No, it just means that he fits the profile of a potential fraudster. We have seen fraud perpetrated by 80-year-old grandmothers and 18-year-old teenagers, anyone can defraud - it just happens that these are the characteristics of the most common fraudsters in Africa.

In all frauds there are 'red flags' or warning signs that you should be looking out for, such as behavioral changes and lifestyle changes, which should then stimulate you to look into the person's new Ferrari or strange behavior.

In the African cases the top-3 red flags were

1. Living beyond their means
2. Unusually close associated with a vendor
3. Financial difficulties

As an organisation you need to have the proper checks and balances in place to prevent fraud and please remember that internal controls do not = fraud prevention! A best practice fraud prevention program consists of nine building blocks of which one of them is internal controls. So if you have controls in place you may still be lacking in the other eight areas.

If you do not have all nine building blocks in place you are missing out on a great opportunity to save 5% of your organisation's annual revenues. That's the huge financial loss that fraudsters take from organisations every year. Prevention is better, and cheaper than cure!

The report concludes with the following fraud prevention checklist that is designed to help organizations test the effectiveness of their fraud prevention measures.

Test your Fraud Prevention levels here:  or  ...

1. Is ongoing anti-fraud training provided to all employees of the organization?

- Do employees understand what constitutes fraud?
- Have the costs of fraud to the company and everyone in it — including lost profits, adverse publicity, job loss and decreased morale and productivity — been made clear to employees?
- Do employees know where to seek advice when faced with uncertain ethical decisions, and do they believe that they can speak freely?
- Has a policy of zero-tolerance for fraud been communicated to employees through words and actions?

2. Is an effective fraud reporting mechanism in place?

- Have employees been taught how to communicate concerns about known or potential wrongdoing?
- Is there an anonymous reporting channel available to employees, such as a 3-party hotline?
- Do employees trust that they can report suspicious activity anonymously and/or confidentially and without fear of reprisal?
- Has it been made clear to employees that reports of suspicious activity will be promptly and thoroughly evaluated?

3. To increase employees' perception of detection, are the following proactive measures taken and publicized to employees?

- Is possible fraudulent conduct aggressively sought out, rather than dealt with passively?
- Does the organization send the message that it actively seeks out fraudulent conduct through fraud assessment questioning by auditors?
- Are surprise fraud audits performed in addition to regularly scheduled fraud audits?
- Is continuous auditing software used to detect fraud and, if so, has the use of such software been made known throughout the organization?

4. Is the management climate/tone at the top one of honesty and integrity?

- Are employees surveyed to determine the extent to which they believe management acts with honesty and integrity?
- Are performance goals realistic?
- Have fraud prevention goals been incorporated into the performance measures against which managers are evaluated & which are used to determine performance-related compensation?
- Has the organization established, implemented and tested a process for oversight of fraud risks by the board of directors or others charged with governance (e.g., the audit committee)?

5. Are fraud risk assessments performed to proactively identify and mitigate the company's vulnerabilities to internal and external fraud?

- Yes or No?

6. Are strong anti-fraud controls in place and operating effectively, including the following?

- Proper separation of duties
- Use of authorizations
- Physical safeguards
- Job rotations
- Mandatory vacations

7. Does the internal audit department, if one exists, have adequate resources and authority to operate effectively and without undue influence from senior management?

- Yes or No?

8. Does the hiring policy include the following?

- Past employment verification
- Criminal and civil background checks
- Credit checks
- Drug screening
- Education verification
- References check

9. Are employee support programs in place to assist employees struggling with addictions, mental/emotional health, family or financial problems?

Yes or No?

10. Is an open-door policy in place that allows employees to speak freely about pressures, providing management the opportunity to alleviate such pressures before they become acute?

Yes or No?

11. Are anonymous surveys conducted to assess employee morale?

Yes or No?

The above questions may sound simple enough but you need to be critically honest with yourself.

A few years back we were dealing with one of the large banks and management said their staff were all intelligent and knew what fraud was and the difference between right and wrong. We convinced management to do a 'dip-stick' test so a survey was emailed to staff where this question was posed:

What is fraud? Is it a) unlawfully taking R10, b) taking R100, c) taking R1000, d) taking more than R10 000 or e) all of the above?

The correct answer is obviously e) all of the above, yet they got varied answers! This was management's wake-up call because they now knew that their initial assumptions had been wrong and that they needed to educate their staff on a regular basis. 'Regular' doesn't mean every ten years or after a fraud is detected - it means monthly initiatives in order to prevent the fraud or to detect it as quickly as possible!

The goal is for you to tick every block above in the affirmative - if just one block is not ticked this could be your 'Achilles Heel' that the criminal exploits in order to defraud you.

If you would like to download the complete report you can do so [here](#)

Copyright for the above Fraud Prevention Checklist belongs to:



**New COSO research study - Fraudulent Financial Reporting: 1998-2007,
(which is an update on the previous COSO study issued in 1999, Fraudulent Financial
Reporting: 1987-1997)**

COSO has released a new research study, Fraudulent Financial Reporting: 1998-2007, that examines 347 alleged accounting fraud cases investigated by the U.S. Securities and Exchange Commission (SEC) over a ten-year period ending December 31, 2007. It provides an in-depth analysis of the nature, extent and characteristics of accounting frauds occurring throughout the ten years, and provides helpful insights regarding new and ongoing issues needing to be addressed.

- Financial fraud affects companies of all sizes.
- The median fraud was \$12.1 million. More than 30 of the fraud cases each involved misstatements/misappropriations of \$500 million or more.
- There were 347 alleged cases of public company fraudulent financial reporting from 1998 to 2007, versus 294 cases from 1987 to 1997. Consistent with the high-profile frauds at Enron, WorldCom, etc., the dollar magnitude of fraudulent financial reporting soared in the last decade, with total cumulative misstatement or misappropriation of nearly \$120 billion across 300 fraud cases with available information (mean of nearly \$400 million per case).
- The most common fraud technique involved improper revenue recognition, followed by the overstatement of existing assets or capitalization of expenses.
- The SEC named the CEO and/or CFO for some level of involvement in 89 percent of the fraud cases, up from 83 percent of cases in 1987-1997. Within two years of the completion of the SEC investigation, about 20 percent of CEOs/CFOs had been indicted. Over 60 percent of those indicted were convicted.
- Many of the commonly observed board of director and audit committee characteristics such as size, meeting frequency, composition, and experience do not differ meaningfully between fraud and no-fraud companies.
- Twenty-six percent of the firms engaged in fraud changed auditors during the period examined compared to a 12 percent rate for no-fraud firms.
- Initial news in the press of an alleged fraud resulted in an average 16.7 percent abnormal stock price decline for the fraud company in the two days surrounding the announcement.
- Companies engaged in fraud often experienced bankruptcy, delisting from a stock exchange, or material asset sales at rates much higher than those experienced by no-fraud firms.

The COSO study was conducted by four accounting professors: Mark S. Beasley of North Carolina State University, Joseph V. Carcello of the University of Tennessee, Dana R. Hermanson of Kennesaw State University, and Terry L. Neal of the University of Tennessee.

The study updates a previous COSO study issued in 1999, Fraudulent Financial Reporting: 1987-1997

Editor's Note: In the previous report one of the characteristics of the companies that had financial statement fraud was that there was no audit committee or they did not have outsiders or they did not meet regularly. In this report the board and audit committees of the fraudulent companies did all the right things - on paper. They had a paper compliance and ethics program. Just like Enron and Worldcom, who had best practice in terms of corporate governance, but it was all smoke and mirrors with a rotten tone at the top. They simply complied with the letter as opposed to the spirit of the law.

What does your tone at the top & corporate culture look like - smoke & mirrors or integrity?

To download a copy of the report you can do so [here](#).

Who you gonna call?

In my nearly 20 years of being involved with fraud prevention I have worked with lawyers, accountants, ex-prosecutors, auditors and people with police backgrounds yet many of them lacked the skills necessary to successfully prevent and detect fraud.



*"It was definitely the perfect fraud...
unfortunately they hired the perfect investigators."*

Some were good at investigating fraud while some were bad. Most, however, had very little skill or motivation to prevent fraud. An investigator has a very different mindset - his or her goal is to find the evidence and lock up the fraudster. Yet the next logical step from the investigation is to correct the root cause that allowed the fraud to take place and to feed these learnings back into the prevention program. This never gets done in the majority of investigations and that is why organisations are doomed to keep having the same frauds repeat over and over.

At some of our clients we deal with the risk manager, internal audit manager or finance manager who understands the importance of prevention and we get hired to implement the fraud prevention program - and then the liaison task (between Exactech and the client) gets delegated to the investigator and our progress hits a stumbling block. The investigator simply doesn't understand prevention or lacks the motivation

(Cartoon source: Michael Comer, Maxima)

to ensure 100% commitment to working with us and making things happen internally.

Another problem is that in South Africa the forensic industry is totally unregulated, so investigators are free to set their own standards and, most importantly, their own ethics. We have seen many botched investigations because organisations hired the 'cheap' PI instead of the CFE! On one case the PI took just a few days to get the evidence while we took two weeks - the difference was that the PI's evidence could not be used in court as he obtained it illegally. (We have often been called in to clean up a mess that was created by the inexperienced forensic auditor).

Organizations should therefore be hiring forensic people (external consultants or when filling internal positions) only if they have some form of international accreditation, such as the ACFE.

At Exactech we hire only people that are CFE's or who are at least members of the local chapter and are studying to attain their certification.

You wouldn't go to doctor that hadn't had formal training would you? So why hire a fraud examiner that has had no formal training or accreditation from a reputable organisation!

If you're in a Fraud-Jam contact us - [Jonathan](#) - [Antonio](#) - [Mario](#)

System Defrag: Electronic Evidence Friend or Foe?

Antonio Poee - Director: Exactech

In our recent pubcast, we discuss an issue paper by the South African Law Reform Commission on the review of the law of evidence. We touch on quite a few pertinent issues relating to this topic. One of which is the impact of searching for electronic evidence after a suspect has run a defrag utility. There has been much speculation about the real impact of a system defrag. I will try to explain this in very simple terms.

Firstly, let's look at the idea behind the defrag process. It is not intended to simply "wipe out every data block previously occupied by data". The purpose is to make data access easy and fast, thus enhancing overall performance of your PC.

So, think back when the standard hard disc drive on a work computer was about 20GB. This meant that if you wanted to defrag, the system would use data blocks occupied by previously deleted data and overwrite them/destroy potential evidence in the process of reorganizing a user's scattered data. This is because the drives were small and there was not enough empty blocks to play around with.

With new 3 digit GB or even TB drives, there is ample free space to use when running a defrag. It is therefore more common to recover deleted data from a defragmented modern big drive.

In short, it's all about the amount of unallocated/free space available for the system to use when reorganizing data, and the volume of user data to regroup.

What this then means is that organisations need to develop/formalise their incident response strategies so as to ensure that there are no delays in preserving potential electronic evidence. Computers must be seized and forensically imaged immediately after an incident has been identified. The idea is not to give the crooked employee any time to defrag the system (or manipulate data in any clever way) as this may reduce chances of recovery of any 'deleted' data.

If you wish to hear or download the full pubcast, click [here](#)

If you wish to post your interesting technical question please visit us [here](#) or email Antonio directly at antonio@exactech.co.za.

How HOT is your hotline?

Jonathan Le Roux, Exactech Fraud Prevention Solutions

You know what you know. You know what you don't know.

But you don't know what you don't know!

Hotlines / Disclosure Lines / Ethics Lines are tools that help organisations to 'know what they don't (yet) know'. They are powerful tools if developed, implemented, managed, monitored and assessed regularly that can serve as a true value creator in an organisation.

Most organisations have a hotline now, but few hotlines are effective, largely due to:

- **Lack of communication** e.g. not included in induction program, hotline info printed very small in publications
- Hotline service is **not the core business of the service provider** e.g. providing the hotline service as a 'wedge' to get into the organisation for other services
- Hotline seen as an **'image detractor'** (make the company look worse) e.g. don't advertise as belief is business image/reputation/brand diminished by it
- **Poor or no hotline service management** e.g. being issued with a 0800 number and a few posters, with no further support by the hotline provider to ensure the success of the hotline service.

From a risk management / corporate governance perspective having the inclusion of your hotline information in your Corporate Report looks impressive to your shareholders or the Board, but that might be where the hotline stops.

Do you know how many calls you received last month? How many of those calls resulted in reports? What is your hotline costing you per month? When last was your hotline reviewed by an independent party?

If you don't know this, then maybe it's time to take stock.

At Exactech Fraud Prevention Solutions, we have recognised that 'people get good at what they do well, consistently'. One of our services in our Fraud Risk Management suite is to assist organisations by implementing both (1) An **effective hotline management service** and (2) A **sustainable awareness and communication program**, being one of the nine fraud prevention building blocks you need to effectively manage fraud.

"As Exactech is a truly South African Fraud Solutions brand – seriously, just take a look at our website - where X does mark the spot in fraud solutions, we have acquired a 40% stake in Be Heard™ (a division of Quiver Management Solutions (Pty) Ltd) who are hotline specialists," says Antonio Pooe (Founder and Managing Member of Exactech).

"This synergistic collaboration means that an organisation who implements a hotline service with Be Heard™, automatically gets to utilise the expertise, knowledge and experience of Exactech to ensure the implementation of an effective and sustainable hotline management program," says Brian Adams (Chief Executive of Be Heard™, who was previously the founder and CEO of Tip-Offs Anonymous).

If you are part of the C-Suite, an owner, a manager, a fire-fighter or President and you have a hotline, maybe it's time you got somebody independent in to review how hot your hotline really is.

For more information please visit [Exactech](#) or [Be Heard](#).

Editor's note - Some organizations have told us "It's not our culture to have a fraud hotline", yet these same organisations have ghost purchasers, security guards, CCTV, access control, and/or electric fences, depending on the industry.

All this is screaming 'WE DON'T TRUST OUR STAFF/CUSTOMERS!' yet they don't want a hotline because 'it will give the wrong impression'!

My question would have to be 'What are skeletons do they have in their closet?!'

Isn't it time your auditor got a Coach?

As I sit here observing the next group of Internal Audit Technicians (IAT) Learnership completing their Training Module 8 on Fraud Risk, I can't but help to wonder, will they be adequately prepared to deal with an environment where fraud is a commonplace activity?

They are mostly young and inexperienced and will be entering a world where they have through their own upbringing respected their elders and the wise. They have been (hopefully) raised on the core

values of self-discipline, honesty and accountability as children through either parental figures or mentors in the respective communities within which they live.

But the community at large is a different place to the world we work in and will test the mettle of the next IATs who will be placed in or at various organisations throughout South Africa and some will be asking questions of the members of management who may very well be the masterminds of the next TravelGate or Tannebaum or Tenderpreneur occupational fraud scam.

So how do we prepare the next generation of auditors to not succumb to the 'fobbing off' by management through what appears to be a 'plausible' explanation to an audit observation or finding? How do we ensure that they remain professionally skeptical? How do we ensure that their objectivity and independence is not impaired?

Simple really, why not hire a Coach!

Yes, you heard right, a Coach. Every successful high-performance team has a coach, assistant coach and then a support team consisting of various specialists like psychologists, doctors, sport-kit management, etc.

The new breed of auditors coming into the working world of today need to be equipped to deal with the future world of tomorrow. They need to be guided and mentored on the various aspects of business and how to cope in a business world.

Some of the questions I would be asking if I was your Risk and Audit Coach, would be:

1. How does your auditor feel about the organisation they work for? Why?
2. What other attributes / skills / knowledge does your auditor have that can enhance or add value to the audit execution?
3. Do you really know what motivates your auditor?
4. How well do you know the people in audit?
5. What does your auditor or audit team mean to you?
6. How often do you actively engage with your auditor or audit team from a non-work perspective? (I am referring to regular 1-on-1 sessions here)
7. What does the internal audit brand stand for (a) for you (b) for your client/management?
8. What is your audit mandate?
9. Do you see that internal audit adds value in your organisation? Or is it a tick-box function?
10. Do you see that you have a future here as an internal auditor? Why?

Before you build and prepare the auditor of tomorrow, you need to understand the person first.

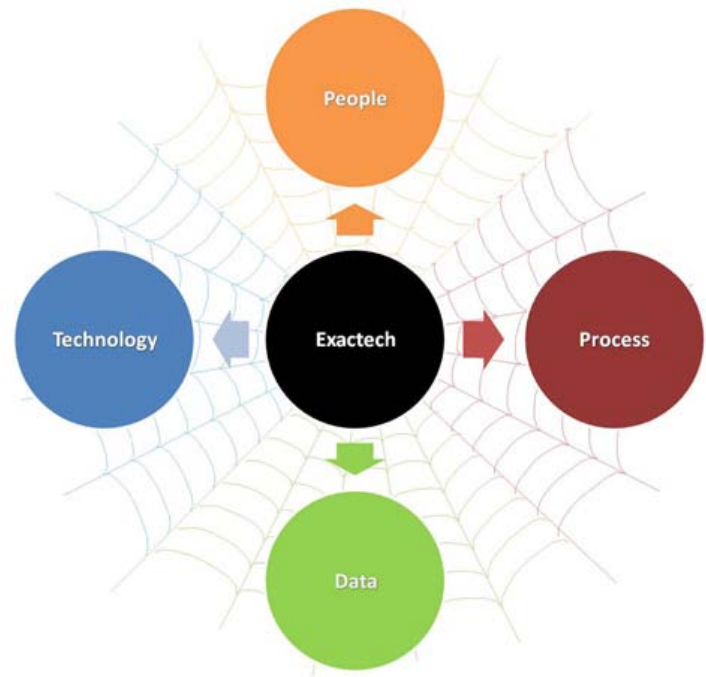
Your objective might be to complete the audits in the approved timeframe per your audit plan or based on your risk prioritisation schedule, but if you do not have the heart and mind of that auditor before you put them on the 'playing field', you do so at a lose-lose situation – loss to you (which includes the organisation) and a loss to that person.

As an organisation, you view your business primarily from four aspects, namely:

- People
- Process
- Data
- Technology

In 80% of our fraud 'root-cause analyses' we find that the 'people' element was the root cause of the fraud. This is not to say that the other three elements are not important - on the contrary - all four business elements are important as are all nine fraud prevention building blocks.

People have a direct impact on controls because it's people that override controls or ignore controls, it's people that decide whether to obey policy or not, it's people that decide whether to implement what they learnt in the training workshop or to stick to their old ways.



Fraud is committed by people.

Because of this, your auditor (and you) needs to know more about people and how they behave. Critical to the potential uncovering of fraud or other associated irregularities is the equipping of the auditor in understanding 'what makes people tick in business' and what they will encounter from people (management) when they are encroaching on their turf. This skill and knowledge will assist in the creation of the next generation auditor.

At Exactech Fraud Solutions, we firmly believe that there are four components that underpin a sustainable fraud risk management solution and the 'People' part of that is core. If you get this wrong by not investing properly because you don't see the need for a Coach, you have just reduced the impact of the next generation auditor.

Remember the Baby-Boomers are gone (born between 1946-1964), Generation X'ers (born between 1965-1977) are in charge (for now).

The future lies in Generation Y'ers (born between 1978-1994).

Are you getting the future of audit fraud-ready with basic people skills and knowledge?

Every team needs a coach. Do you have one?

HOW CAN ON-SITE DOCUMENT DESTRUCTION HELP YOUR COMPANY REDUCE THE RISK OF FRAUD.

It is becoming increasingly common to hear reports of records containing private client information being disposed of in an improper manner. Patient files found in landfill, personal information recovered in trash bins and company designs leaked to competitors. These are risks faced by organisations on a daily basis. In order to mitigate these risks, companies need to ensure they have adequate control over their information within the office environment as well as externally, on its way to being recycled.

Cleardata offers a risk management solution to its clients, by ensuring that all confidential information is shredded at the client's premises before being recycled. Documentation is securely stored within the office environment in our locked containers and shredded on-site in our mobile shredding vehicle before the recycling process begins. Cleardata guarantees that no information will leave your premises in a complete form and ensures that all shredded paper will be recycled immediately after the destruction process is complete. By giving the client the ability to maintain control over its sensitive information at each transaction point, Cleardata has helped to significantly reduce the risk of fraud within the corporate sphere.

Every organization that possesses or has access to confidential information, such as payroll records, medical and financial records, and other personally identifiable information, needs to protect the privacy of its customers and employees.

Due to the rapidly increasing incidence of identity theft – and the awareness of protecting personal information – laws and regulations regarding the protection of personal information have been in place throughout the United States, the United Kingdom, most EU members and Australia for a number of years. South Africa has lagged somewhat in all-encompassing privacy protection legislation. In late 2002, the South African Law Reform Commission gave notice of a project to begin work on drafting South Africa's first piece of legislation dealing exclusively with Privacy Protection. It seems likely that the final Act will be reviewed by parliament later this year.

Cleardata's operations are certified by NAID –the global super advisory body for the document destruction industry, with audits taking place on an annual basis. This certification brings peace of mind to clients, both local and international as it ensures conformity to the most stringent of US and European standards, and results in a service that is fully compliant with Protection of Personal Information Act soon to be in place in South Africa.

“Organisations need to understand the importance of concealing the privacy of their information within the organisation. This means protecting the information from outsiders as well as employees. Information needs to be protected while in the office environment and before being disposed of.”
Gianmarco Lorenzi: Founder and Managing Director of Cleardata.

Cleardata is South Africa's first and only Nationwide provider of secure, on-site document destruction solutions for the corporate environment. Headquartered in Gauteng, with regional offices and representation across 8 provinces, they are uniquely positioned to provide clients with a complete solution to the delicate task of protecting sensitive client, staff and business information. Cleardata are proud to boast a service that is ISO 9001 certified and Carbon Neutral, achieved primarily through the 'Food & Trees for Africa Offset Scheme'. For more information on Cleardata's on-site document destruction service please visit www.cleardata.co.za

Fraud and Ethics Training & Awareness:

The majority of our fraud and ethics training is done for membership organisations such as SAICA, CIMA, IIA, ACFE and CIMA. Here is a photograph of Antonio at the Sandton SAICA workshop...



and Jonathan presenting at one of the IIA Internal Auditor Technician training courses...



Over the last twelve months we have done workshops in South Africa, Namibia, Botswana, Lesotho and Tanzania. When last were your staff members exposed to a fraud prevention workshop? I love this quote: ***"If you think training is expensive, how much do you think ignorance costs?"!***



The Institute of Internal Auditors South Africa

4-day How to detect & prevent occupational fraud: 15 - 18 November 2010, Bedfordview, Johannesburg

Why these courses are important...

“If you were to ask a group of typical accountants what deters fraud, they would respond in unison: ‘Internal control!’

Using this logic, companies with adequate controls would not have fraud. But they do, time & again”

– Joe Wells, founder of the ACFE

General Course Outline...

The success of a fraud risk management program relies on an organisation implementing a dynamic and sustainable anti-fraud strategy.

We unpack the nine best-practice fraud prevention building blocks and then show how to get management buy-in. We use case studies; show DVDs and use practical exercises to ensure that workshop attendees are ‘edutained’.

Some past delegate comments...

- ***Made me aware of the fraud risks to my clients and myself.***
- ***I definitely enjoyed every minute and it was a big eye opener.***
- ***Thank you for an excellent course - I was so impressed by your knowledge, presentation skills and enthusiasm.***
- ***I am now able to go back to my company and plug the gaps.***
- ***Made me realise that fraud is possible even if there are internal controls.***
- ***It created a strong awareness in me on how to prevent and detect fraud.***
- ***Mario has inspired me to go back and enhance our anti-fraud initiatives.***
- ***Integrity and values must be the cornerstones to any organisation.***
- ***The seminar was excellent and I greatly enjoyed the examples you provided of moral relativism, as well as the areas of vulnerability.***

To register please click [here](#) or contact Jenine or Maria at the **Events Department on:**

Tel: +27 (0)11 450 1040, email: events@iiasa.org.za

The publishers believe that the information in this Fraud Prevention Newsletter is correct. However, it is published without liability upon the publishers for loss of any kind occasioned by any person or organisation acting or refraining from acting as a result of information contained herein. Contributors' opinions and statements should not be considered an endorsement by Exactech for any policy, programme or service. Subscribers, readers and users of all related services have been made aware that this publication is not a substitute for specific professional legal and other advice. Provided that **Mario Fazekas (e-mail: mario@exactech.co.za)** is notified of the intended use and on condition that acknowledgement is made to Exactech and the authors, you are welcome to reproduce articles.