Editorial…

Welcome to the Spring 2016 issue!

It looks like 2016 will end as a bumper year for the fraudsters. Cifas' (The UK's Fraud Prevention Service) annual report on UK fraud trends reveals 25% increase in recorded fraud. South Africa is never far behind the rest of the world, and in some cases we beat the rest of the world especially with things like fraud cases, so in SA the increase could be much more!

The top three increases were in remote banking fraud, identity crime and organized crime.

We get to speak to many people – either at clients, while travelling or at training events and we’ve noticed that many people are being defrauded by the same old scams. It seems like some people don’t read papers, don’t attend training courses or simply don’t think it’ll happen to them.

The scams we’re talking about are the following:

- **We paid money into your account in error, please will you refund us.** The cheque is stolen and once you refund the money is gone and you’re left with a bounced cheque.

- **Change of bank details scam.** The fraudsters get hold of your client list and they email or fax the clients with an official-looking letterhead requesting your banking details on their system be changed. They even supply a cancelled cheque and/or bank letter.

- **The Nigerian 419 scam.** You receive an email from a person asking for your help – they have millions of dollars and they need a bank account to transfer it to and if you help them you can have some of the money.

- **Executive Impersonation scam.** Your finance manager receives an email from the most senior person in your organization asking for money to be urgently transferred.

In This Edition:

- The Rogue Employee
- Spot Checks / Surprise Audits
- 11 Sad Words about Fraud
- 6 Common Myths about Fraud
- Fraud Awareness Training
- Some Training Courses we’ve done in 2016
- SAICA Espresso Shots
- The IIA 4-day Fraud Prevention & Detection Training Course
- Who do You Trust to Protect You from Fraud?

Enjoy!

Mario Fazekas, Editor
Email: mario.fazekas@exactech.co
Mobile: + 27 (0)83 611 0161
www.exactech.co
Mistakes and accidents do happen. In the corporate world, diligence and verification procedures can go wrong and the end result may be a harmless product recall with some short-term damage to the company’s reputation.

Some organisations admit fault, fix the problem, pay the fines, if any, and move on, but others start the blame game as they don’t want to admit failure of their processes and their favorite target to blame is the lone ‘Rogue Employee’.

Let’s look at a four recent examples:

1. **Société Générale** – Jérôme Kerviel was criminally convicted, as the rogue trader, for engaging in trades which cost the bank €4.9bn back in 2007 and 2008.

   However, in a French labor court decision in 2016, it noted, “**Société Générale could not pretend it hadn’t long been aware of the unauthorized trades** conducted by Mr. Kerviel”. The judges went on to note, “The bank therefore can’t argue that Mr. Kerviel was at fault when it ‘previously tolerated similar practices… and Kerviel’s managers were aware of his activities and turned a blind eye as long as he made money for the bank’.”

**Solution:** What has the bank done to ensure there are no more incidents of this nature? Among other things, the bank has changed its remuneration policies - it no longer rewards only financial performance, but also the methods and conduct by which this is achieved and the risk management put in place to attain these goals. It has also taken steps to change the Bank’s culture by strengthening its "risk culture", with a significant campaign to raise the awareness of all the Group’s employees in relation to fraud risk.
2. **Toshiba** - Toshiba allegedly overstated operating profits by $1.9 billion over seven years going back to 2008.

An interesting article on the Toshiba fraud scandal said that *"Japanese cultural traditions might have led to the breakdown in the corporate tone at the top".*

An 82-page summary of the investigation's findings stated that the fraud started with senior management pressuring employees who interpreted that as implicit directions to cook the books. Many employees were ultimately involved in the huge scheme and cover-up. The report noted that Toshiba's accounting department *"deliberately provided insufficient explanations to auditors, with the intention of carrying out a systematic cover-up."* The report also stated that there *"existed a corporate culture at Toshiba where it was impossible to go against the boss' will"*, referring again to general Japanese culture.

**Solution:** Disciplinary steps for accounting irregularities were taken against 26 senior officials, such as a one-day suspension from work (*"What's the difference between that and a paid holiday?"* asked one employee), pay cuts (the head of Toshiba's financial affairs department was slapped with a pay cut amounting to a maximum 1/60th of a monthly salary) and reprimands (*"please don't do it again"?*), while 7800 employees were retrenched due to ‘restructuring’! (This is a ‘solution’…?!)

3. **Volkswagen** - it was discovered in 2015 that for nearly a decade, VW programmed software to activate pollution controls in its diesel vehicles only during emissions testing. This was done on 11 million diesel vehicles sold worldwide.

According to Michael Horn, VW’s US chief executive, this was caused by *“a couple of software engineers”* who did it for unknown reasons. Chris Collins, a Republican representative from New York, responded to this statement by saying: *“I categorically reject everything that VW is saying about a couple of rogue engineers. Either Volkswagen management is incompetent or they are complicit in a massive cover-up that is continuing today.”*

Fortune Magazine stated that *“VW’s ability to rebound from this cheating scandal hinges on the company’s willingness to address the culture [of arrogance] that enabled it”*, which has been acknowledged by Müller, the new CEO.

**Solution:** The Times reported that Volkswagen’s new CEO is working to change the company culture, replacing "yes" men in favor of people who "follow their instincts, and are not merely guided by the possible consequences of impending failure".

4. **Wells Fargo** – *“Wells Fargo CEO Defends Bank Culture, Lays Blame with Bad Employees”* – It’s like putting all the blame on the child and totally ignoring the parent’s duty for teaching, nurturing and disciplining the child. *“When we first started looking at it, we didn’t think it was anything other than rogue junior players and a few rogue managers,”* says someone involved in the bank’s internal discussions.
So what happened? Wells Fargo employees created over 2,000,000 fake cheque and credit card accounts, over the past 5 years, using customers’ identities to boost their sales numbers due to a high-pressure sales culture.

Wells Fargo’s chairman and chief executive, denies that the company’s culture is obsessed with nonstop selling that ran amok. “Could we have done more, faster, better? Of course,” he says. Mr. Stumpf also says he “feels accountable” but adds that some employees (5300!) didn’t honor the bank’s values.

End result – the world’s largest bank fires 5300 employees for fraud and the exec in charge walks away with R1.7bn! This fraud is either due to 5300 ‘rogue’ employees or a company culture that encouraged unethical behavior.

Solution: Wells Fargo outlined a series of new actions to strengthen culture and rebuild trust - they have eliminated product sales goals for Retail Banking team members; they have started sending confirmation after new accounts have been opened and they are providing refunds to clients who were charged fees on the fake accounts. I wonder if this will be enough…?

Wells Fargo & Co. Chairman and Chief Executive John Stumpf, under fire for the bank’s sales-tactics scandal and his own handling of its fallout, has eventually stepped down from both roles after initially refusing to do so as he did nothing wrong. Bernie Ebbers, the former CEO of Worldcom, and Dennis Kozlowski, the former CEO of Tyco, both used that excuse and it didn’t work with the judges and shouldn’t work here either.

Conclusion:

So, from the above examples we can see that the ‘rogue’ employee is generally a dangerous myth because all employees work and operate within an organisational context. For a rogue employee to exist, and operate, there has to be a lack of organisational (managerial) oversight. As Susan Silbey (Professor of Behavioral and Policy Sciences at Sloan School of Management) describes it “there has to be a rotten barrel to create a rotten apple”.

In a sense, the rogue employee argument is a tacit or implicit admittance that the organisational control system is broken with a resulting toxic culture, and blaming a “rogue” employee is simply a poor attempt to cover systemic issues.

The common word used in all the above examples was ‘CULTURE’ and to quote Peter Drucker (management consultant, educator, and author),

“Culture eats strategy for breakfast”

In the next issue we will be looking at ‘culture’ and what organisations should be doing to evaluate and rectify their corporate cultures to ensure they don’t end up like the above organisations.
9 top officials sacked after Dubai ruler's spot check reveals empty desks

Sheikh Mohammed bin Rashid al-Maktoum, Dubai's ruler, carried out an unannounced early morning inspection of several civil service departments only to find empty desks.

A day after the inspection, Sheikh Mohammed ordered the retirement of nine members of Dubai Municipality's executive management, including directors and assistant director-generals. There were many other employees absent but the exercise was intended to "send a message that timeliness starts at the top and we won't go after employees when their bosses aren't there."

You may be thinking that being dismissed for tardiness (being late) is very harsh and that the punishment should fit the crime. Well, small unethical behaviors tend to lead to much bigger unethical behaviors!

The 2016 ACFE global fraud survey showed that in 38% of frauds the perpetrator had exhibited at least one of these seemingly non-serious ethical misconducts such as tardiness.

The other inappropriate workplace behaviors are intimidation, excessive absenteeism, sexual harassment, excessive internet browsing and browsing of inappropriate websites.
Surprise visits / surprise audits are a necessity. So many frauds have been concealed because external and internal auditors told clients which branches they would be auditing and when.

If I’m responsible for the petty cash and you tell me you will be coming to check the petty cash on Monday morning, do you think it will balance? **Of course it will!** And when you leave, if I’m a fraudster, I will resume my ‘borrowing’ until the next time you phone me to tell me you are coming to count my cash and I will simply replace what I have borrowed.

**Discipline starts at the top.** In so many organisations the root cause of the fraud is a bad boss. The boss, by mocking the code of ethics, the hotline and other anti-fraud measures, can encourage some subordinates to defraud when the opportunity presents itself. Other bosses are hands-off and they spend more time having lunches and playing golf than managing their teams.

A speech by Stephen Cutler, the then Director, Division of Enforcement, U.S. Securities and Exchange Commission, gave a speech entitled "**Tone at the Top: Getting it Right,**" where he listed eight things organisations should be doing to ensure strong ethics and antifraud programs and one of them is - **hold all of your managers accountable for setting the right tone.**

"**That means disciplining or even firing them when they have failed to create a culture of compliance. Human nature being what it is, there will be those who break the rules. But if managers don't do enough to prevent those violations, or let them go unaddressed for too long, then they should be held responsible - even in the absence of direct involvement in those violations.**"

We see this so many times in our clients – the perpetrator is disciplined, fired and/or prosecuted by nothing happens to the manager. The manager is paid to manage the department and that means being aware of what’s going on.

At one client we were doing a fraud risk assessment and we asked managers to tell us about their subordinates. In about 80% of the cases all the managers could tell us was if they were male or female, tall or short, young or old. We asked if they were married, lived in a small house or a mansion, walked to work, drove a bicycle or owned a Ferrari – the answer “I don’t know”!

We recommended to the CFO that all managers needed to get to know their subordinates more and suggested they meet their subordinates, one-on-one, once a month in the canteen or other private area and have an informal chat. They should not talk business but just chat in general.

Many employees say that their employer or boss doesn’t care about them so this exercise (if it’s sincere) should change that perception. One of the root causes of fraud is a person being disgruntled and thinking no one cares about them.

Our client encouraged managers to have these monthly meetings and within three months staff morale had improved, hotline calls had picked up and one manager discovered a fraud. He offered the employee a lift home as his car was in the panel beater and the house was huge. He reported this to IA and upon investigation they found the clerk had been misappropriating client funds to fund a lavish lifestyle!
11 SAD WORDS ABOUT FRAUD

This article was originally written by David L. Cotton, CPA, CFE, CGFM and we have shortened it and added our comments to it.

Fraud has been with us since the serpent told Eve it would be okay to take a bite out of that apple in the Garden of Eden. Since then, fraud schemes have multiplied, prospered and grown in ingenuity and deviousness.

Fraud is not diminishing, and we need to acknowledge that fraud will not go away. Some experts believe that less than 1 in 10 frauds is ever discovered.

Four sad words precede every fraud
At some point, prior to an organization becoming a fraud victim, someone in that organization uttered the phrase, “It can’t happen here.” Often, those words followed someone else’s — usually an accountability professional’s — urgings to strengthen control procedures.

We’ve all heard the arguments against spending resources on control processes and procedures:

1. “It’s too expensive;” Organisations lose an average of 5% of annual turnover to fraud each year!!! Surely spending 0.1% of annual profit to prevent this huge loss would make good business sense?

2. “We don’t have enough people to segregate duties;” Co-source with specialists! In-house can be expensive as you have salaries and other perks to pay while with outsourcing you lose control – co-sourcing makes so much sense. Our clients hire us on retainer and we work for them however many days they require per month. Win-win!

Here’s a quote from John T. Parish, CPA, director of internal audit at FirstCity Financial Corp:

Many companies have gone on "crash diets," using outsourcing to shed noncore tasks such as internal audit to outside vendors. In the process they’ve lost day-to-day control over a department to a professional service firm and often gained new problems. Proposed solutions from outside consultants—strangers to the organization—don’t always work. As a result, quality, profitability and employee morale can suffer. Co-sourcing is another way to get a company into shape, trimming costs while maximizing internal audit capabilities and still retaining control.
3. “That control stuff is a bunch of bureaucratic red tape;” Is that really the type of things some executives say about compliance and controls?! Indeed it is. Here’s a quote from Richard Kovacevich, the former CEO / Chairman of Wells Fargo…

“I think what’s happening today, is that they [banks in general] are getting rid of sales staff and investing in technology and so on, in order to pay for compliance. It is staggering. In our bank there are probably close to 10,000 compliance people…It is absurd that we are investing that kind of money on compliance.

It’s obvious from what happened there that their compliance program was just a smoke screen with little or no management support. Otherwise how do you get 5300 unethical, non-compliant employees doing what they did over so many years (2010-2016)?

4. “We only hire and only do business with trustworthy, honest people; so our organization is different.” Wishful thinking! If only it was possible to identify and hire only honest employees. There are two types of criminals:

- The career criminal who does fraud full-time and most probably has a criminal record – this person should be detected before hiring, if you HR function does proper background checks.

- Then we have the situational criminal. This person is honest today but then the three elements of the fraud triangle kick in; pressure, opportunity and rationalization and the person starts to defraud. This is where internal controls such as management reports, data analytics and the hotline should detect the anomalies or unusual behaviors.

Seven even sadder words follow every fraud
Immediately following the discovery that one of those trusted associates has made off with valuable assets, leaving heartache, pain and disarray where those assets used to be, the victims always shake their heads and say, “We didn’t think it could happen here.”

Victims of fraud will always admit that they should have listened to those accountability professionals.

Too bad there is not a way to promote that “better-safe-than-sorry” attitude in organizations before the damage is done. Prevention is better than cure but so few organisations are willing to be proactive and spend a few cents of prevention and early detection and so they end up spending hundreds of thousands, if not millions, of Rands on investigations.
6 COMMON MYTHS ABOUT FRAUD – part 5

If not debunked, they can obscure the existence of white-collar crime.

(Based on an article written by Joseph Wells and printed in the AICPA’s [American Institute of Certified Public Accountants] Journal of Accountancy).

A solid auditing or accounting background is helpful in uncovering white-collar crime, but it’s not the whole answer. Auditors now turn up only about 20% of the frauds detected. Most fraud cases are discovered by accident or are revealed through complaints by co-workers.

Globally, employees are stealing as much as $3.5 trillion annually, according to estimates from the Association of Certified Fraud Examiners (ACFE), which specializes in fraud detection and deterrence. They also show that the average bank robbery nets the criminal only about $3,200, but the average bank embezzlement is $125,000. ‘Internal Controls’ do NOT equal ‘Fraud Prevention’, so to meet their expanded responsibilities to uncover fraud and control it, CPAs need to know more about fraud prevention. In particular, they need to debunk these six myths about fraud.

MYTH #5 - THE AUDITOR CAN’T DO A BETTER JOB IN DETECTING FRAUD

There are a number of reasons auditors don’t detect fraud. Some frauds are well beyond the scope of the audit. Some are too well concealed. Some are too small. But perhaps the greatest reason is that the evidence is not reflected in the financial statements. International Standard of Auditing, ISA 240, states under paragraph 2: “When planning and performing audit procedures and evaluating and reporting the results thereof, the auditor should consider the risk of material misstatements in the financial statements resulting from fraud or error.”

And ISA 240 also requires the auditor, when planning the audit, to discuss with other members of the audit team the susceptibility of the entity to material misstatements in the financial statements resulting from fraud or error and to make various inquiries of management relating to fraud and fraud risks.

There are essentially two types of frauds on--book and off-book. The former consist of typical employee frauds, such as embezzlements, phony expenses and ghost employees on the payroll. Although sometimes difficult to detect, on-book frauds at least have audit trails. Off-book frauds consist of kickback and bribery schemes, conflicts of interests and similar offences. These frauds or illegal acts tend to involve upper levels of management, they involve much larger amounts and they are not normally detected by traditional audit procedures.
Detection of off-book frauds can be a particular problem since they are outside the scope of traditional audits. Investigation of these frauds usually requires extensive experience in interview, interrogation and collection of evidence.

In fraud examination methodology, a profile of a suspect is developed by looking at the high-risk factors of not only the organization but also its personnel. In many cases the auditors know they have a problem but not who was responsible. A Certified Fraud Examiner’s first step would be to interview the company employees and then determine which employee/s demonstrated the ‘red flags’ or motivators for fraud. Once the suspect/s has been identified, it becomes a simple matter to gather evidence of his guilt.

Auditors can learn from this methodology. Those who wish to uncover fraud must be aggressive and should not be reluctant to ask questions about fraud. All too often, other employees know about or suspect fraud but they may be afraid to report their suspicions.

Management’s role in this regard is to create an environment in which fraud awareness becomes everyone’s responsibility and any employee can furnish information without fear of reprisal. Many companies now have developed reward policies for “whistleblowers” and have cut their losses significantly.

Auditors should understand the environment when designing their tests.

**Fact**

Of all the myths, this one is the biggest whopper! The auditor can do a much better job in detecting fraud **if adequately trained** to recognize fraud, is willing to accept the responsibility to find fraud and is then prepared to design the work program to look for fraud.

As Steve Albrecht says, “**Most people, including accountants and auditors, wouldn’t recognise a fraud if it hit them between the eyes**”. But it needn’t be so. The technology, the techniques, and the tools exist to defend against, and defeat, fraudsters. There are products and services on offer to protect against all types of fraud. Given that the technology exists to protect ourselves on a corporate level, we should try to understand why we remain defenseless.

Why has so little been done, and why have the available defensive technologies not been deployed to the extent they should have? Two reasons – **apathy** (tomorrow’s another day) and/or **arrogance** (fraud happens to other people).

On a corporate level, the danger of procrastination is potentially very dangerous. Procrastination is an addictive drug, & incessant postponement catches up with us sooner or later, generally at a much higher personal or financial cost. **Remember that fraud affects salary increases, bonuses & jobs!** Each problem we choose to ignore ends up costing us more in the long run. We must not allow fraud losses to be added to the list, not when we have before us a way to avoid the dangers & expenses.
Fraud Awareness Training cuts Fraud Losses by 50%

- Do your staff members know which fraud risks threaten your organization?
- Can they spot the red flags of embezzlement, billing schemes, and payroll fraud?
- Do they know how to report suspicions about these and other wrongdoing?

If your answer to any of these questions is “no” or “don’t know,” you’ve got plenty of company. More than 50% of all organizations have no employee fraud awareness training in place—despite the fact that nearly one-half of all frauds that are detected are discovered by employee tip! (Association of Certified Fraud Examiners Report to the Nations 2016)

But things are changing -- fast. Today, with fraud and cybercrime worsening, more and more organizations are implementing employee fraud awareness training—to get early notification of fraud … mobilize response measures … and eliminate control weaknesses that enable fraudsters to do their damage.

They are doing it by having experienced anti-fraud experts who use a concept called ‘Edutainment’ – educating by using humor, games, practical exercises & surveys to create powerful & engaging training to get employees up-to-speed on fraud prevention & detection.

By implementing regular fraud awareness training you can see a huge return on investment in terms of protection against the exploding fraud and cyber-criminal problem …

Not to mention the 50% reduction in fraud losses that results from implementing employee fraud awareness training, according to the Association of Certified Fraud Examiners.

<table>
<thead>
<tr>
<th>Control</th>
<th>Percent of Cases Implemented</th>
<th>Control in Place</th>
<th>Control Not in Place</th>
<th>Percent Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotline</td>
<td>48.6%</td>
<td>$100,000</td>
<td>$245,000</td>
<td>59.2%</td>
</tr>
<tr>
<td>Employee Support Programs</td>
<td>44.8%</td>
<td>$100,000</td>
<td>$244,000</td>
<td>59.0%</td>
</tr>
<tr>
<td>Surprize Audits</td>
<td>28.9%</td>
<td>$97,000</td>
<td>$200,000</td>
<td>51.5%</td>
</tr>
<tr>
<td>Fraud Training for Employees</td>
<td>39.6%</td>
<td>$100,000</td>
<td>$200,000</td>
<td>50.0%</td>
</tr>
<tr>
<td>Fraud Training for Managers/Execs</td>
<td>41.5%</td>
<td>$100,000</td>
<td>$200,000</td>
<td>50.0%</td>
</tr>
<tr>
<td>Job Rotation/Mandatory Vacation</td>
<td>14.6%</td>
<td>$100,000</td>
<td>$188,000</td>
<td>46.8%</td>
</tr>
<tr>
<td>Code of Conduct</td>
<td>69.9%</td>
<td>$140,000</td>
<td>$262,000</td>
<td>46.6%</td>
</tr>
<tr>
<td>Anti-Fraud Policy</td>
<td>39.0%</td>
<td>$120,000</td>
<td>$200,000</td>
<td>40.0%</td>
</tr>
<tr>
<td>Management Review</td>
<td>53.3%</td>
<td>$120,000</td>
<td>$200,000</td>
<td>40.0%</td>
</tr>
<tr>
<td>External Audit of ICOFR</td>
<td>59.3%</td>
<td>$140,000</td>
<td>$215,000</td>
<td>34.9%</td>
</tr>
<tr>
<td>Internal Audit/FE Department</td>
<td>66.4%</td>
<td>$145,000</td>
<td>$209,000</td>
<td>30.6%</td>
</tr>
<tr>
<td>Independent Audit Committee</td>
<td>53.2%</td>
<td>$140,000</td>
<td>$200,000</td>
<td>30.0%</td>
</tr>
<tr>
<td>Management Certification of F/S</td>
<td>58.9%</td>
<td>$150,000</td>
<td>$200,000</td>
<td>25.0%</td>
</tr>
<tr>
<td>External Audit of F/S</td>
<td>76.1%</td>
<td>$150,000</td>
<td>$200,000</td>
<td>25.0%</td>
</tr>
<tr>
<td>Rewards for Whistleblowers</td>
<td>7.4%</td>
<td>$119,000</td>
<td>$155,000</td>
<td>23.2%</td>
</tr>
</tbody>
</table>

November 13-19 2016 is Global Fraud Awareness Week – what have you got planned for your organisation?
Some of the training courses we delivered in 2016:

The training room at Mercedes Benz where we delivered a 1-day fraud awareness course for dealer and head office staff on ID Theft & Body Language. No, the red Mercedes wasn’t for me!

The two Answer Champs who won the 3-day fraud class quiz – an extra 10 marks each that went toward their IAT (Internal Auditor Technician) fraud module marks.

At the SARB, attendees at a 2-day Anti-fraud Agent course worked in departmental groups to come up with fraud prevention tools for their respective departments.

Management of the Lesotho Electricity Company, working in groups to solve a problem at our 4-day Fraud Prevention & Detection course.
We delivered a 2-day ‘Advanced Forensics’ course for bica (Botswana Institute of Chartered Accountants) members in Gaborone. People learn best when doing, so here the delegates are working in groups to solve a fraud investigation problem…

We are also doing 90-minute Espresso Shots for SAICA members. We have already done a few with good feedback.

These are the remaining ones for 2016:

Practical Fraud Risk Management

Johannesburg – 4th November 2016
Polokwane – 15th November 2016
Nelspruit – 17th November 2016
East Rand – 25th November 2016

"I have been practicing as a CA for almost 20 years and endured many hours of the most boring CPD lectures imaginable. Mario is definitely a breath of fresh air. The lecture was both informative and very entertaining and an absolute pleasure to attend. If more lectures could be this good I am sure all practitioners would look forward to attending their CPD hours".

- Peter Carlisle CA (SA)
Here are the dates for our popular 4-day *Fraud Prevention and Detection* CPD course run by the IIA...

- 29 Nov – 02 Dec 2016, Bedfordview, Johannesburg
- 05 Dec – 08 Dec 2016, Cape Town

Why these courses are important...

According to the 2016 ACFE global fraud survey, the average organisation loses 5% of its annual turnover to fraud!!

General Course Outline...

- The success of a fraud risk management program relies on an organisation implementing a dynamic and sustainable anti-fraud strategy.
  - We discuss criminology theory and the fraud triangle.
  - The three categories of occupational fraud are examined.
- 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 contact Jenine, Lister or Maria at the *Events Department on:*

Tel: +27 (0)11 450 1040, email: events@iiasa.org.za
Who do you trust to help protect your organisation's profits from Fraud?

“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

Internal Controls ≠ Fraud Prevention!!

Every organisation has internal controls but they don't all have fraud prevention!

Exactech specializes in helping private and public sector organisations to implement best-practice anti-fraud initiatives based on the ten fraud prevention building blocks.

Fraud is present in almost all businesses, with only the 10 fraud prevention elements to keep it in check. When some of these elements are missing or are circumvented, frauds can quickly grow to shocking proportions.

Exactech specializes in:

**Fraud Risk Management:**
- Code of Ethics Review / Creation
- Data Analytics
- Ethics Training
- Fraud Awareness Training
- Fraud Risk Assessments
- Hotline Management
- Policy Reviews

**Digital Forensics:**
- Computer/PDA/Cell phone imaging
- Cyber Forensic Training
- Discovery & examination of deleted & Formatted data
- Password & data recovery
- Vulnerability Audits
Contact details

As usual, we welcome your feedback, ideas for future issues and suggestions of how we might make the newsletter more useful for you. Please send your comments to:

mario.fazekas@exactech.co

You can also use this email address to tell us if you would like to receive this free newsletter in future.

Individual contact details are as follows:

**Antonio Pooe** (Cyber Forensics)
Email: antonio.pooe@exactech.co
Tel: +27 (0) 11 475 2525
Cell: 072 781 4157

**Mario Fazekas** (Fraud Risk Management)
Email: mario.fazekas@exactech.co
Tel: +27 (0) 11 475 2525
Cell: 083 611 0161

The publishers believe that the information in this Fraud Risk Management 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.fazekas@exactech.co) is notified of the intended use and on condition that acknowledgement is made to Exactech and the authors, you are welcome to reproduce articles.