



EXACTECH

Fraud Prevention Solutions



FRAUD PREVENTION NEWSLETTER

June 2008

Editorial...

Welcome to the June newsletter!

We've had a busy month in respect of fraud awareness events; Antonio Poe delivered a presentation on Continuous Controls Monitoring at the 7th IIA SA & ACFE Fraud Conference at Emperor's Palace, I delivered a presentation on the importance of an ethical culture at the SAICA KZN Networking Breakfast held at the Sun Coast hotel, and we attended a procurement fraud breakfast at Bowman Gilfillan's Sandton offices.

In this issue we have the second part of the Fraud Deterrence Lifecycle article focusing on the Prevention element. The article explains what should be in place while next month we will show how best to implement these prevention building blocks.

There is definitely a hunger for information on how to successfully fight fraud but there is also more than enough information available out there as can be seen from the small snapshot above of what awareness initiatives were being run last month. How come then is there still so much fraud?

Well, I've just finished reading a motivational book called "**212° the extra degree**", obtainable from Successories, and I think it provides the answer. Water boils at 212 degrees Fahrenheit (100 degrees Centigrade) and the book discusses how just one degree can make a huge difference. Applying one extra degree of temperature to water means the difference between something that is simply very hot and something that generates enough force to power a train – an effective metaphor that ideally should push us to make the extra effort in every action we undertake, including our fraud

prevention efforts. The point we are making here is that we have seen so many organisations implementing a code of ethics, for example, and then not regularly communicating the code or implementing a hotline and then not having it professionally managed on a day-to-day basis. They are simply not going the extra degree that will ensure success.

How would you rate your fraud prevention program – is it simply sitting at 99 degrees or lower, or has it reached the magic 100 degrees Centigrade?

If you want your anti-fraud program to 'boil' you need to do three things:

1. Implement all nine building blocks – it's not a menu where you can choose what appeals to you – all the elements work together to give you the 'deterrence' factor.
2. Ensure that all stakeholders know the elements are in place and what their responsibilities are.
3. Test the various initiatives to see if they are achieving their aims.

Yes, it will cost money to implement and test the nine building blocks but we will demonstrate in the next newsletter issue how you can achieve ROIs (Returns on your Investment) of up to 30:1.

You will also be getting more information on each of the nine building blocks as we will be publishing articles, written by specialists, starting in this issue with Johan Kruger and Antonio Poe's respective articles. ■

Mario Fazekas, Editor

Email: Mario@exactech.co.za

Mobile: 083 611 0161

White Collar Crime, a Stitch in time...

-by Johan Kruger, Bowman Gilfillan

Considering the amounts of money spent on the investigation of serious economic crime and related issues by both the private and public sectors in South Africa, and the cost of the losses suffered as a result thereof, fraud prevention has received only a fraction of the attention that it deserves. It appears that entities in the private sector and government alike, still only react to fraud once the losses have already been incurred, rather than to approach the issue of economic crime proactively. This appears to be the fact **despite the references to fraud prevention** and corporate governance in the Public Finance Management Act, the Prevention of Organised Crime Act, the King II Report on Corporate Governance and other Acts and publications.

Experience has shown that, in 99% of cases where entities have suffered significant losses, it can be attributed to a failure of internal controls. More often than not, the control in question is a basic and simple measure that was never implemented or was neglected. Fraud flourishes in an environment where it is tolerated and where the measures introduced to combat it are not strict enough.

The Institute of Internal Auditors defines Fraud Prevention as follows: "Fraud Prevention consists of the actions that are taken to discourage the perpetration of fraud and limit the organisation's exposure, or risk, if fraud should occur."

The Bowman Gilfillan White Collar Crime team has been instrumental in developing and implementing fraud prevention measures for a number of our clients. It may be useful for our readers to understand our approach to fraud prevention practices.

Fraud Prevention in any entity is best served by a **comprehensive fraud prevention strategy that usually consists of a number of components**. The first is the Fraud Prevention Policy that should be adopted by top

management and should be widely publicized within the entity. The second is the fraud prevention toolkit that consists of a variety of action plans that are to be implemented within the organization and that are all aimed at preventing fraud in one way or the other. The third is a rollout plan that contains a schedule of when, where and how each action plan will be implemented.

The fraud prevention policy should reflect management's attitude to fraud. It should be noted that there can be no grey areas where fraud is concerned. The only possible attitude that management can have towards fraud and other economic crime is one of zero tolerance. Fraud prevention means creating a work environment that values honesty. Top management can create such an environment by setting an example of honesty and fairness in their daily interactions with their peers and subordinates. If management is seen to be acting with diminished integrity, they should expect their subordinates to assume that that is the norm to be followed in the particular entity.

The fraud prevention toolkit usually consists of practical action plans that may be implemented to reduce fraud. The action plans may be divided into the following four categories:

- >> The Fraud Prevention Policy and Employee Sensitisation;
- >> Managing Human Resources;
- >> Managing the Fraud Risk; and
- >> Managing Information Technology Risks.

Under the first heading, the fraud prevention policy should be adopted by top management in a manner that leaves no doubt in the mind of employees that the contents thereof should be taken seriously. Wide internal publicity should be given to the event and reinforcement should take place on a regular basis. Other measures that may be implemented to heighten employee awareness are staff sensitisation and ethics workshops, employee participation schemes, the implementation of a fraud hotline, internal publication of fraud related matters and the circulation of the zero tolerance message via management road shows, particularly in an organisation that is decentralised into different

cities or provinces. The management of **human resources** with regard to fraud prevention may consist of, inter alia, the following elements:

- >> Proper employee vetting and background checks on potential employees. This is known as the first line of defence against fraud, the principle being that, if you do not employ fraudsters, you shouldn't have a fraud problem.
- >> The adoption of a code of conduct that is tailored for fraud prevention.
- >> The implementation of gift registers and registers of private interests.
- >> Service contracts designed to provide certain legal recourse to the employer in cases of fraud or suspected fraud.

The management of the **fraud risk** contains action plans that have specific bearing on the risk and internal control environment of the entity. Measures that have proved to be effective in this regard are:

- >> Fraud risk assessments and grading of certain positions as high risk areas;
- >> Surprise audits on randomly selected business areas;
- >> The implementation of certain fraud prevention measures with regard to procurement procedures;
- >> Creating supplier & trading partner awareness;
- >> Fraud training for management;
- >> The implementation of a Fraud Response Plan; and
- >> The identification & control of environmental risks that are unique to that particular business or industry.

Addressing risks unique to **information technology** are proving to be of particular importance in the new millennium. A number of highly effective action plans may be introduced to address these risks:

- >> The implementation of a comprehensive information technology policy granting the entity full access to all systems and limiting the right to privacy of employees with regard to the computer systems of the entity;

- >> Regular monitoring of systems and the creation of exception reports;
- >> Data mining for the purposes of fraud detection; and
- >> Information security and the creation of fire walls and other security measures.

It is of great importance to note that every entity is unique with regard to fraud prevention and that each strategy should be designed to address the particular risks of that entity. Apart from possibly saving a business from imploding in "Enronian" fashion, the most important benefits of a successful fraud prevention strategy are:

- >> Cost savings & increased revenue & profits;
- >> The limitation of reputational risk; and
- >> A positive and ethical work environment and high employee morale.

Experience has demonstrated that the cost associated with the drafting and implementation of an entity-wide fraud prevention strategy is in most instances less than the losses incurred in one serious incident of fraud. In the case of fraud, it is truly better to drain the swamps than it is to fight the crocodiles. ■



This article is based on Johan's article that appeared in the 'Nature of Law', Edition 1 2008, Bowman Gilfillan's client publication.

FRAUD DETERRENCE

Part 2 of our article on fraud deterrence where the focus will be on the **Prevention** part of the lifecycle.



Fraud prevention is 80% of the solution.

According to Toby Bishop, the past president of the ACFE, *“a major change is taking place in the strategy for fighting fraud. The emphasis is shifting from 20% prevention/deterrence and 80% detection/investigation to the opposite ratio. The high returns on investment being achieved by companies that fight fraud vigorously suggest that an ounce of prevention is worth at least a pound of cure.*

There should be an objective evaluation of an entity’s fraud prevention processes with prompt action to fix gaps and then annual testing and ongoing fraud education and training”

Traditionally, forensic investigations have been the main focus with prevention playing second fiddle. This is now changing as investigations are being perceived as the ‘black hole’ where money can disappear with minimal perceived value. Many companies are now saying things like, *“We get more bang for our buck out of prevention than investigation”*, with one of the main gripes being, *“Investigators can’t seem to translate their findings into process improvements”*.

Fraud Prevention Building Blocks

Fraud prevention should be looked at holistically and is presented here as sequential building blocks (based on the ACFE’s fraud prevention checklist) making up the program:

Risk Assessment	Accountability	Controls
Data Analytics	Policy	Whistle-blowing System
Value System - Ethics	Recruitment	Training & Awareness

We will start with the two cornerstones and work our way up the other blocks:

The code of ethics is the one critical cornerstone where no short-cuts should be taken. The success or failure of a fraud prevention plan depends primarily on the culture of the organization, and a sustainable Ethics Management Program will ensure that ethics is top-of-mind within the company. Merely having a code of ethics is not sufficient so cutting-edge companies are designing and implementing training around the code, bringing what is often a dormant item to life. Far too often, the code lies buried in an organisation’s employee training manual and is handed out to new employees on their first day on the job and then forgotten about.

Training & Awareness is the other critical cornerstone and by linking fraud awareness training to the code of ethics sends a strong message and reinforces what is considered appropriate behavior by the company. Training needs to happen annually and it must target existing employees as well as new recruits. The training should also bring in the whistle blowing system and how it works, the various policies, procedures and other related documents, as well as roles and responsibilities. The training should be ‘edutaining’, meaning it should inform

and entertain as this is the best way for people to learn and retain what they have learnt.

Recruitment - The best indicator of future performance is past performance so it is crucial to conduct background checks on new employees and existing employees being promoted to positions of trust. Professional background checks as well as exit interviews, can uncover a whole host of problems and integrity concerns.

Data Analytics – Many organisations have been scared away from data analytics for the following reasons:

- There are too many software products to choose from
- Obtaining data is difficult
- The exercise takes too long, Involves too many analysts, costs too much
- The results tend to be extremely lengthy and difficult to understand

For the above reasons, a recent solution has been created (called Continuous Controls Monitoring), that uses automated, pre-defined analytic tests to critical control points within specific business process areas. By automating sophisticated analytics and embedding audit "best practices" in organisations' business operations, management receives timely notification of anomalies and control breaches, mitigating risks of ineffective or missing controls within application systems. Business process owners receive timely notification of control breaches, can quickly review quantified exposure of business risk, and can drill down to specific exceptions and transactions to resolve potential problems before they escalate. As a result, organizations can better assure compliance, contain costs, and minimize losses.

Whistle-blowing System – Many frauds are known or suspected by both insiders and outsiders. The challenge for management is to encourage these 'innocent' people that disclosing what they know or suspect is their responsibility and is very much in their own interest. The organisation's anti-fraud culture and reporting processes can be a major influence on the whistleblower but it is often fear

of the consequence that has the most influence. To the whistle-blower the result of speaking out can be traumatic, ranging from being dismissed to being ostracized by colleagues.

Policy – The aim of a corporate fraud policy is to demonstrate to all stakeholders that the company is taking the threat of fraud and dishonesty seriously. By issuing a detailed policies (such as a Fraud policy, Whistle-blowing policy, Reward policy, Fraud response plan, Code of conduct, etc.) it clearly sets out what is considered to be dishonest, warns any potential wrongdoers that the consequences of being caught will be serious and explains each process. The effect therefore will be to deter any potential wrongdoers thus resulting in reduced losses from fraud and reduced costs in respect of investigating any wrongdoing.

Risk Assessment - Management should assess the vulnerability of the organisation to fraudulent activity every 18 – 24 months. This is traditionally done by evaluating the type of fraud risk, the potential impact of the fraud, the likelihood of its occurrence and the pervasiveness of the risk. Fraud can occur in any organization but the degree and detail involved in the risk assessment should obviously be based on its size and complexity.

Controls – After the fraud risk assessment results have been perused, management should determine whether there are controls in place to mitigate the identified fraud risks or if additional emphasis should be placed on existing controls. Where controls are not present, management should design & implement antifraud controls and / or even re-engineer the process, to address the identified fraud risks.

Accountability – Dishonest employees may not commit a fraud if they know the organization has an oversight and confirmation process. After giving the code of ethics to all employees (in both hard and soft copy if possible), require that they sign a statement that says they have read and understood the code's requirements and will comply with them. This eliminates the excuse of ignorance. Staff with an anti-fraud responsibility, such as management and fraud champions, also needs to be held accountable for their responsibilities and performance. ■

THE FOLLOWING FRAUD TRAINING COURSES ARE BEING RUN IN 2008:

The Institute of Internal Auditors South Africa (all hosted in Johannesburg)

- 1-day Fraud Awareness - **7th July 2008**
- 2-day Prevention & detection of white collar crime - **8-9 Sept. 2008**
- 4-day How to detect & prevent occupational fraud - **27-30 Oct. 2008**

For more information please contact:

Jenine Dresse

Tel: (011) 450 1040

Fax: 086 685 0161

Email: seminars@iiasa.org.za

www.iiasa.org.za

The Chartered Institute of Management Accountants (CIMA):

- 2-day 'Catch Fraud before it Catches You' Mastercourse
Western Cape - 10-11 July 2008
Johannesburg - 16-17 July 2008
- 1-day Fraud Prevention Mastercourse
Botswana – 18 September 2008
Zambia – 16 October 2008

For more information please contact:

Tsholofelo Dihutso

Tel: +27 11 268 2555

Fax: +27 11 268 2556

Email: tsholofelo.dihutso@cimaglobal.com

www.cimaglobal.com

What delegates can expect from these courses:

- Practical examples of fraudulent items will be examined.
- Local and international fraud case studies will be discussed in order to ascertain best practices.
- DVD's will be used to introduce the audience to a mob boss, ex fraudsters, and whistleblowers.

ACL for Management Seminar

The ACL management seminar will provide management with the necessary background to successfully assess the deployment of ACL in your organization. Participants will be made aware of the management environment that they must create to maximize the return on their investment in ACL. Several issues, such as establishing relations with data providers, understanding the potential value added by data analysis software, & the qualitative & quantitative evaluations of ACL implementation will be covered in depth.

1st July 2008 @ Glenhove, Rosebank.

Registration: 7:30, Seminar: 8:00am – 9:30am

Bookings:

CQS Website: www.cqs.co.za

Email: info@cqs.co.za

Phone: Linda Wilson @ 011 507 0042

Thank you to one of our past delegates, Viv Jones, of the Hub Trading Company, Durban, for the following poem...

**Fraud the unseen reaper
The business not any clearer
Denied of its very importance
Not believing in its existence**

**Tis' management must bear the blame
For not detecting - what a shame
But for us the Internal team
We must persist and find the scheme**

**Stop the reaper spoiling the plan
Use the 'four-ways' that sees the scam
Detection, Investigation - Correction is fine
But Prevention will stop future crime**

**Call Centre, Hot Line to complain
Raise awareness that's the aim
To encourage feedback of the scams
To save the company thousands of Rands.**

Continuous Fraud Auditing / Monitoring

This is a summary of the presentation Antonio Poe delivered at the 7th IIA SA & ACFE Conference held last month at Emperor's Palace and attended by over 350 delegates.

In an on-line poll conducted by Knowledgeleader in 2007, just 4% of respondents said Yes, their organisation has automated its fraud monitoring, with a whopping 88.4% saying 'No' and 4.6% saying they were Not Sure yet now is the time for organisations to make progress with their fraud prevention programs & continuous monitoring is one of the most effective tools available to detect fraud as the following quote shows:

“Now is the time for corporations to fix fraud and controls weaknesses. Nearly all financial executives (90 percent) report a cultural change among U.S. business leaders toward institutional integrity and fraud prevention as a result of the recent fraud scandals.”

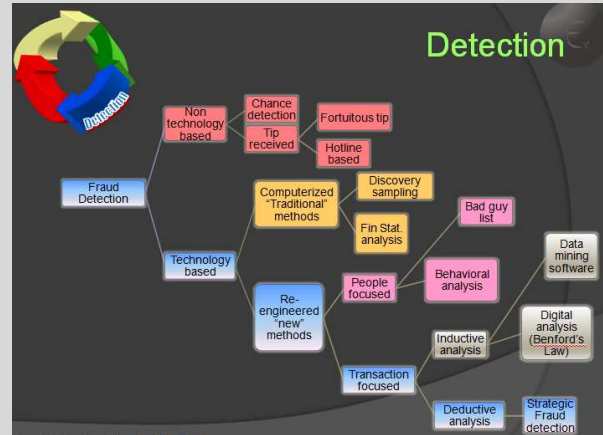
“Today, continuous monitoring is a mature process that allows companies to automate controls testing and get real-time visibility into their financials. Smart compliance officers & corporate executives are adopting these processes and technology.”

- 2007 Oversight Systems Executive Report on Sarbanes Oxley

The following diagram, compiled by Dr Steve W Albrecht & Conan C Albrecht in their 'Strategic Fraud Detection: A Technology-Based Model' paper, demonstrates that there are basically two methods of detecting fraud:

- Non-Technology based – this would be reactive, hoping that employees who see fraud actually report it.
- Technology based – this would be proactively looking for fraud with 'Transaction focused' being the most effective. 'Inductive analysis' is the shotgun approach where an organisation uses off-the-shelf software to look for red flags of fraud while 'Deductive analysis' would be the use of data analytical software, such as ACL, to

look for specific frauds that could occur or have occurred in the past in your particular industry.



Most organisations use ad-hoc data analytics, normally during an audit or after a fraud has been discovered. This is often too little too late as the money has already been taken. Continuous Fraud Auditing, however, notifies the relevant persons within the organisation in real time of any suspicious transactions or anomalies. This could be via an email or SMS, and the transaction can be examined the very next day in order to ascertain whether it was correct detection.

With Continuous Fraud Auditing and Monitoring the organisation can use their business intelligence to be more efficient and more profitable. It is not just an audit tool – it is also a management tool that allows each department to see just what is happening in their respective areas and to respond to the early warnings.

One of the big plusses with continuous fraud monitoring is that the organisation doesn't need to rely on teams of expensive analysts – the organisation retains control of the process and the reporting is easy to understand.

Organisations that implement continuous fraud auditing and monitoring are at the cutting edge of technology with a huge advantage over competitors who are not. But hey, let us not tell you how great this is, let some users do that from various industries such as Retail, Healthcare, Mining and Telecoms:

*"With continuous monitoring software, we have been able to automate the review of 100 percent of our payment transactions. This provides us with an added degree of certainty over the effectiveness of controls of our payables which is critical as we move towards SOX 404 certification. **This solution has resulted in the identification of duplicate payments which are five times the total cost of implementing the software.**"*

- Gary Silsbe, Director of Operational Excellence, Telus

*"As a result of the ACL CCM system we have been able to identify and implement significant improvements to our organisation's system of internal controls. **We have identified invalid transactions in real time and prevented financial loss.**"*

*Our continuous control monitoring system provides the **ideal tool for both management and internal audit** to continually monitor the effectiveness and levels of compliance with controls established to manage financial risks associated with the business."*

- Terrence Spencer, Regional Audit Manager, Xstrata

*"As a result of the continuous monitoring of data, we have improved merchandise turnover rates, reduced our payment time to suppliers, and **saved the company millions of dollars.** These are critical issues for any retail business, and ACL Audit Analytics has made it possible for our company to gain a competitive advantage by solving them."*

- José Dimas Gonçalves, CFO, Sonae Distribuicao

"The next step for HCA's audit group is maximizing ACL as a value-added tool in continuous monitoring, using data from company sub-systems and third-party vendors. And we are starting to make that happen at HCA with amazing results."

CCM enables us to institute auditing procedures that are driving best practices throughout the company."

- Kevin McMahon, Vice President, Internal Audit & Chase Whitaker, Director IA & Dept Lead – Continuous Audit, HCA

*"CCM has enabled us to take control of our data and gain a deeper understanding of trends in Managed Care Organization plan payments. As CHS Audit Services gained more experience with ACL's software, the project completion time dropped by 50 percent, even as its scope continued to expand. **This three-year Managed Care Payment project has been so successful, the Variance Summary Report was nicknamed 'the treasure map'.**"*

- Linda B. Franklin, Senior Auditor, Carolinus Healthcare System. ■

If you missed the conference & would like a free 30-minute presentation on Continuous Fraud Auditing & Monitoring contact either:

Antonio Poee

Cell: 072 781 4157

Email: antonio@exactech.co.za

or

Mario Fazekas

Cell: 083 611 0161

Email: mario@exactech.co.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 (Cell: +27 (83) 611 0161 or 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 in whole or part.