

**DEVELOPING A FRAUD PROFILE METHOD
- A STEP IN BUILDING INSTITUTIONAL GOVERNANCE -**

Paper presented at

Ethics and Integrity of Governance Conference: A Transatlantic Dialogue

Organised by:

*Study Group on Ethics and Integrity of Governance, of the
European Group of Public Administration*

Hosted by:

*The Public Management Institute
Katholieke Universiteit Leuven*

2-5 June, 2005

By

Peter Steane
*Macquarie University
Australia*

And

Robert Cockerell
Ernst and Young
Australia

Correspondence:

Professor Peter Steane

Graduate School of Management,

Macquarie University, Ryde, NSW 2109, AUSTRALIA

Telephone: + 612 9850 9136; Email: peter.steane@mgsu.edu.au

DEVELOPING A FRAUD PROFILE METHOD

- A STEP IN BUILDING INSTITUTIONAL GOVERNANCE –

Fraud is a particular crime. It does not usually involve violence but can have devastating effects on the lives of people and the efficacy of institutional governance. This paper presents macro and micro level cases in a collaborative practitioner–academic project to develop a more robust method for understanding, investigating and preventing fraud. It is part of the contribution to ethical and effective institutional governance.

The investigative methodology arises in part from two sources: Ernst and Young experience in investigations and fraud prevention across different sectors in an economy and across cultural and legal jurisdictions, and academic expertise in ethics and management systems. It contributes an analytical tool more proactive in managing risk within public and private enterprises, which is more strategic, focused and cost effective.

Normative crime analysis indicates that there is **motivation, target and opportunity**. Fraud preventative theory usually attacks the problem by attending to these areas. We extend this trilogy approach with two further categories that need to be considered in respect to fraudulent behaviour. The first category is **fraud indicators**, otherwise known as “alerts”, which are behavioral clues that can be observed that consistently accompany fraudulent behaviour. The second category is **fraud methods**, which are generally similar: payroll (ghost employees), accounts payable (employees authorizing payment to themselves or companies they have created), accounts receivable (falsification of bank reconciliations). The final category is what can be described as **fraud consequences**, which are systemic, business or operational impact on enterprises of the fraudulent behaviour.

We argue that the three components of normative fraudulent behaviour (motivation, opportunity and suitable target) combined with three extended categories (fraud indicators, methods and consequences) *extends the theory on both understanding and investigating fraud*. The cases used in this paper are discussed in terms of these categories. The resultant Analysis Led Fraud Assessment (ALFA) methodology utilises the process of investigation, induction (gathering of information) and deduction (analysis) to develop fraud profiles, and can be used to provide a focused, cost effective response to fraud prevention and detection by enterprises. In the end, it contributes to the efficacy of institutional governance.

Our conclusion is that understanding and preventing fraud is a necessary but not sufficient condition to managing risk. Ethical cultures and leadership are just as important in building better institutional governance.

Understanding Fraud

Fraud is a particular crime. It does not usually involve violence to another person, but does harm a system or corporate entity, which in turn can harm people. Fraud can be defined as dishonest actions to steal or misrepresent or gain advantage at the expense of others or due process. The affects of fraud are widespread: companies can suffer financially, financial results and company value can be distorted, people can be disadvantaged and loose employment, to name a few.

This paper argues that motivation, opportunity and suitability of target are the three key ingredients for fraud, and that organizations can act responsibly and proactively by using them as a focus for assessing their risk. What is needed is a more robust methodology that

will identify critical areas of fraud risk within an organization and assist management in assuming their responsibility to proactively manage their risk.

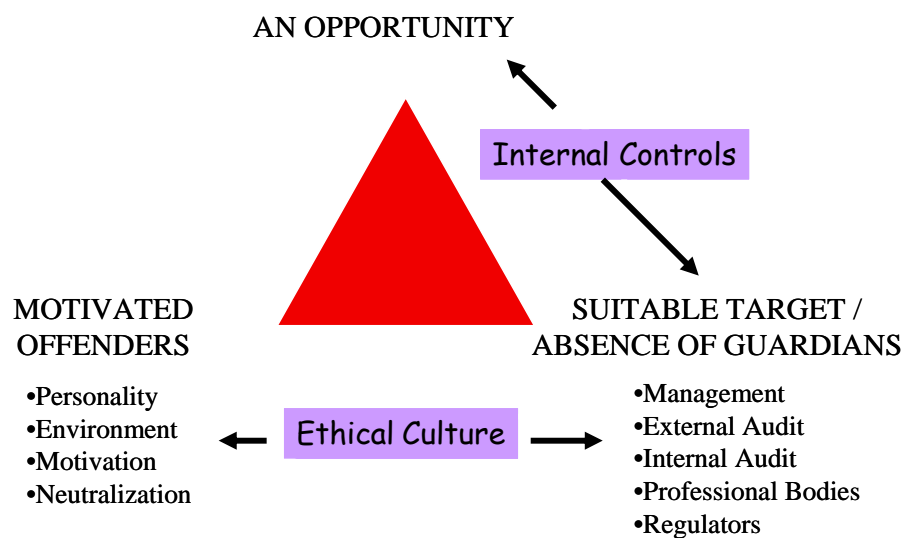
Fraud is not a recent phenomenon in the history of commerce. History is littered with instances of misrepresentation for unlawful gain. Fraud in Australia costs an estimated \$5.88 billion dollars that equates to 31% of all crime (Australian Institute of Criminology 2003). The Association of Certified Fraud Examiners' 2002 Report To The Nation claimed occupational fraud and abuse is estimated to be 6% of revenue. Whilst some argue this figure is exaggerated and that an estimate of 2% is more reasonable, the fact remains the estimates are of considerable concern, particularly as the funds misappropriated come off the so-called "bottom line".

The trilogy of crime analysis indicates that there is *motivation*, a *victim/ suitable target* and *opportunity*. So fraud prevention attacks the problem by attending to these areas. This effort is by a whole range of individual and corporate activity:

- Corporations Law, overseen by The Australian Securities and Investments Commission (ASIC), as well as the Australian Standard AS3806-98 *Compliance Programs*, and others, all aimed at structural efforts to prevent fraud.
- Various government legislations instigated over the recent decade aimed at business and public sector efforts to stem fraud.

These statutes briefly categorize, what Adam Grayer (2000) describes as both legal and systemic initiatives to address the problem as it relates to motivation, victim/suitable target, opportunity (see Figure 1). First, *victims/suitable targets* can be corporate entities, and need to assume greater responsibility in managing risk and establishing fraud prevention measures. Second, *opportunity* exists because of ineffective monitoring systems, poor management, bad leadership, and rotten organizational cultures. When companies and professions face up to rectifying problems – in all its soft and hard manifestations – then it is a step in the right direction. Third, *motivation* is both personal and environmental. Organisations need to increasingly understand what motivational influences operate to result in criminal behaviour.

Figure 1 Three Ingredients of Crime/ Fraud



Graycar (2000)

Generally, fraud prevention efforts, such as the statutes above, are commendable. They are necessary, but they are not sufficient conditions for dealing with the problem. This means attending to *motivation*, *opportunity*, and *targets/victims* is essential to understand the problem and create solutions, but they are never enough in themselves. Better monitoring systems help; stronger legislation assists; ethical leadership builds credibility.

It is internal control mechanisms that mitigate to reduce opportunities for people to commit fraud risk and minimize a company's profile as a suitable target. Similarly, resources and time spent on developing an ethical culture are good long-term investments in minimizing the suitability of a target as well as motivation to offend. Just as each of the trilogy can be the focus of some attention, each one of the three is inter-related to the other dimensions. Just as greater regulation through monitoring and legislation can be encouraged to combat fraud, it is really only a partner to better educative efforts to build ethical organizational climates and better management behaviour. At the end of the day, organizations are increasingly required to take responsibility for the management of their exposure to risk.

When considering the trilogy (Figure 1), *opportunity* usually occurs due to a breakdown in internal control processes. This happens for a variety of reasons: operational expediency, management laziness, through to deliberate intent on the part of someone to defraud the company. Similarly, the suitability of a *target* can be identified for different reasons:

- Simple accidental discovery of organizational weakness (eg, an inadvertent and simple double claim on expenses is later discovered not to be detected), that reveals a systemic flaw in control systems.
- Long-time work experience in the company provides employees with a very good overall understanding of the parameters of internal control strategies, to the extent that fraud can be operationalized safely, without triggering alarms, so long as one remains familiar and within these parameters.

What occurs at one level in the organization, such as the "coal-face", is often not what is management understood was taking place. Internal controls can be breached as a consequence of management strategies seemingly remote from the consequence, such as, operational expediency, unworkable processes, lack of staff, and segregation issues. It can arise that that senior management will no idea procedures are flaunted or disregarded until something happens as a consequence of the procedures not being followed.

Motivation

As stated, there is a range of motivations behind fraudulent behaviour:

- Financial/greed
- Gambling and other addictions
- Revenge
- Maintaining Lifestyle
- Jealousy
- Financial Support for Business
- Personal Debt
- Thrill seeker
- Power Dominance

Each motive is the genesis of diverse patterns of behaviour. It is interesting to see the prevalence of gambling as an increasingly frequent motivation for fraud. One notorious example is the insurance company employee stole \$4.5m over a nine year period of about \$10k per week, simply to support his gambling habit. Another case reports the transport

industry Chief Financial Officer who misappropriated \$20m over three years because of similar addictive reasons.

This paper argues that motivation, opportunity and suitability of target are the three key ingredients for fraud, and that organizations can act responsibly and proactively by using them as a focus for assessing their risk. What is needed is a methodology that will identify critical areas of fraud risk within an organization and assist management in assuming their responsibility to proactively manage their risk.

Fraud Indicators

In seeking to identify fraudulent behaviour within an organization much attention has been focused on fraud indicators which are loosely termed: 'red flags', 'fraud alerts' and 'personal indicators'. Red flags are behavioural clues that may be picked up by managers, colleagues, internal auditors, subordinates that suggests an employee or colleague may be engaging in some form of fraudulent or improper conduct.

Fraud alerts are those unusual occasions and suspicious instances associated with documentation, administration procedures or the general way business is done. These are valuable alerts because they put the person noticing them on guard that something is amiss.

Personal indicators are the private matters of an individual's life that might provide a motivation to commit fraud:

- Significant personal or family problems (health, divorce).
- Failure to take extended and deserved annual leave.
- Domination of specific activities and possessiveness about custody of records or office space.
- High personal debts.
- Extensive gambling.
- Excessive use of alcohol or drugs.
- Always manages to produce good results.

There is a particular skill required to recognize the warning signs within an organization. Basically, it requires good self awareness skills and good skills at attending to irregular or inconsistent or odd circumstances in the work-life of others. Some would call this suspicion, but it is more than simply this. It is the ability to relate work behaviour to a possible cause in private life, to see patterns within events and procedures, and to identify potential causal links to statements and actions. These skills have long been used in psychology and counseling in dealing with *projection* and *displacement*. For managers, the hectic schedule of daily activity focus on outcomes often precludes time and attentiveness to such matters.

The following case provides an insight into fraud through discussing it in terms of motivation , opportunity, suitable target and fraud indicators:

A senior bank manager, with a major bank, misappropriated \$118m over a three-year period. The misappropriated funds were provided to a client, allegedly to construct retirement villages. During the eventual court hearings, it was alleged that the bank manager's motivation was to become the finance manager of the organization created by the client as well as possess a 20% ownership in the business. According to the lending file of the records held by the bank manager concerning this particular client, only \$10m had been authorized.

In order to lend the unauthorized funds to the client, the bank manager breached the bank's existing lending controls. Part of the bank control mechanisms involved the draw down of funds through commercial bill facilities. The procedure for the draw down of the funds were as follows:

1. A form directing the funds to be drawn down on behalf of the client was to be completed in triplicate. This form was to be countersigned by a fellow bank officer who had a direct knowledge of the approval of the loan.
2. The original was to be forwarded to the bank's treasury area, whose officers were to initiate the draw-down and direct the funds to the clients account.
3. The duplicate was to be forwarded to the bank manager's Business Units Ledger clerk who was to record the draw-down of the funds in the Business Units Ledger.
4. The triplicate copy was to be forwarded to the client for their information as to the interest rate and the amount of the funds provided.
5. At the end of the month, the Business Unit Ledger clerk was to reconcile the funds drawn down on the business unit with the bank's General Ledger.

In order to lend the unauthorised amount the bank manager corrupted the existing process by first, placing a false counter signature on the form directing the funds to be drawn down. This false signature was used on over two hundred of the drawn down forms found by investigators. Second, the original draw-down form was forwarded to the bank's treasury with the other forms being disposed of by the bank manager. Third, when the Business Unit Ledger clerk was unable to reconcile the Business Unit Ledger to the bank's general ledger, she was told by the bank manager to pass a control entry to effect the balance.¹

This case can be analysed in terms of motivation, opportunity, and suitable target to provide a fraud profile useful in investigative procedures and managing risk. In terms of *motivation*, the bank manager wanted to leave the bank and believed that the entity his client was seeking to create was his way of securing his future outside the bank. The *target* proved suitable via the commercial bill lending facility. Although the process was designed to prevent fraud, the bank manager was experienced enough to know how to corrupt it. The *opportunity* arose when the previous ledger clerk left the bank and the bank manager offered to train the new one. The training in incorrect procedure allowed him to commit the crime.

The "fraud indicators" included the following the bank manager rarely took leave and refused to go on bank training programs and he refused promotions when offered. The "fraud indicators" also manifested when the authorized lending file had been reviewed by internal audit who identified a number of issues concerning the maintenance of the file including the lack of appropriate security in place. As well, the training of the Business Unit Ledger clerk by the bank manager should have raised some concern, as it blurred the segregation of duties between back office and front office responsibilities. What the case reveals is that motivated people will create opportunities and identify suitable targets, and that they will even manipulate the situation to do this. Furthermore, they will work inside the existing parameters of the risk management strategies.

The lesson for management is that there is a need to be aware of the warning signs and fraudulent indicators can manifest. At the very least, it is incumbent upon senior management to recognize this proactive approach as an important part of their responsibility, in attending to organizational and system vulnerability and managing risk accordingly. One method this paper offers is ALFA and is both flexible and focused in assisting management to identify critical areas of fraud risk and assume their responsibility to proactively manage risk.

¹ The bank manager had told the Business Unit Director that he would teach the ledger clerk how to perform her role.

Developing a Fraud Profile

There are two further categories that need to be considered in respect to fraudulent behaviour. The first category is fraud methods. People often ask which industries are likely to be the most vulnerable to fraud. Experience suggests that any industry type is vulnerable to fraud but that certain types of fraud are more common in particular industries such as construction (where secret commissions and corruption of the tendering process may appear) and insurance (where claims are manipulation).

In relation to fraud however the methods of committing the various types of fraud are generally the same, for example, payroll (ghost employees), accounts payable (employees authorizing payment to themselves or companies they have created), accounts receivable (falsification of bank reconciliations). It is therefore important to include fraud methods when one seeks to identify fraudulent behaviour in an organization.

Another important consideration in the identification of fraud is what can be described as fraud consequences/results. Fraud impact or consequence can be described as the operational and/ or financial impact of the fraudulent behaviour.

We argue that these six components of fraudulent behaviour motivation, opportunity, suitable target, fraud indicators, fraud methods and fraud consequences can be used to provide a focused, cost effective response to fraud prevention and detection. These six components can be brought together to develop fraud profiles. The following cases are discussed in terms of these categories.

Case Studies

Learning from case analysis is a long proven method of successful and innovative professional practice. It was used as long ago as the pre-Socratic philosophers of ancient Greece. The very real advantages to be gained for preventing fraud, apart from the knowledge and concepts developed, are the skills of critical thinking, argument, and improved decision-making, that assist organizations in the prevention of fraud and the overall management of risk. These are crucial skills for both managers and board directors to be proficient in.

Case 1: Magda

This matter concerns the Claims Supervisor of an insurance company. The employee who had worked for the company for fifteen years had a gambling habit which, it was estimated led to losses of about \$15,000.00 per week. In order to support his gambling addiction the employee misappropriated funds from his organization to an amount of approximately \$4.5m. The fraud took place over at least nine years. It was estimated that the employee was taking at least \$10,000.00 per week.

The fraud involved the supervisor re-opening closed insurance claims usually for motor vehicle accidents and then adding an additional party to the accident. The supervisor had opened 15 bank accounts in different names. The supervisor had been able to do this as he utilised a system whereby accounts were opened in the name of children with the supervisor acting as trustee.

The supervisor would approach junior data input operators and direct them to re open an account. Once the account was opened the supervisor would have the operators input information concerning the fictitious third party. This information included the amount to be paid, the method of payment (usually cheque), and the address to where the cheque was to be sent. On a number of occasions the supervisor would use the password and signing authority

of part-time employees when they were not at work. The supervisor would always direct the cheques to the Head Office where he was responsible for receiving the cheques.

The supervisor was causing at least 3 fictitious cheques to be raised per week. As a result the supervisor had to use the 15 false accounts he had developed on a number of occasions. This ranged between 55 to 45 multiple uses of names. As a result of the additional third party being added to the claim this often led to the premium of the insured being increased. The misappropriated money which was at least \$550k per year also led to Victoria being the least highest performer as far cost of claims to revenue.

The supervisors motivation as discussed was gambling. His fellow employees during interviews provided accounts of the supervisor being sighted in gambling venues before work and during the lunch break. The employees also stated that he the supervisor gave the impression that he was a successful punter.

The supervisor when interviewed by investigators stated that he would go every morning to a gambling venue and play the poker machines he would do the same and lunch time and on the way home visit at least two or three venues betting on race horses and also playing poker machines.

Motivation	Opportunity	Suitable Target	Fraud Indicator	Fraud Method	Fraud Consequence
Gambling	Lack of control over counter signing of claims and the ability to re open closed claims and add parties to the closed claim.	Motor Vehicle Accident Claims	Persons allegedly signing claims when not at work	Multiple claims in the names of particular individuals	Poor performance of claims to revenue

Case 2: Leah

The employee was the accounts receivable clerk at a distribution outlet of a major petroleum company. The employee would receive cheques through the mail and cash and cheques over the counter. The employee it was discovered was taking the majority of the cash she received and falsifying month end financial data to conceal the misappropriation.

The employee was responsible for receiving the money, entering receipts onto the debtors ledger and banking of funds received each day.

The correct process was for the employee upon receiving funds to enter the receipt of the funds against each debtor. In order to simplify the checking procedure if any issues were raised in relation to funds received the total receipts, on each given day, were divided into banking batches (this was an operator generated function). The total of these batches was to equal the total of the funds entered on a particular day.

The accounting system generated banking deposit slips divided into the batch amounts created through the system.

A Daily Banking Reconciliation was also required to be completed this document which was handwritten by the employee was designed to record the actual banking batches for each day and the total of funds to be banked.

As the employee was taking cash each day she could not bank the total amount she received. The employee would therefore only use one of the accounting system generated deposits and dispose of the others usually two or three. The employee would then enter one correct banking batch on the Daily Banking Reconciliation however the other two would be false amounts. The Daily Banking Reconciliation, one accounting system deposit listing and cash would then be taken to the Bank.

At month end a reconciliation of the bank statement to the accounting system banking batches would be made. During this process those involved in the reconciliation would check the individual batch amount recorded in the accounting system against the total deposit made to the bank and the Daily Banking Reconciliation. During this process the persons doing the reconciliation would simply check batch amounts and not the dates of the banking of the batches.

In order to cover up her fraud the employee would record on the Daily Banking Reconciliation batch amounts, which she would need to eventually create in the accounting system.

At month end for two days the accounting system would be left open to receive funds through another accounting system used by a large number of outlets. These receipts were titled outstandings. The employee would use these funds to cover her theft in that she would record a higher amount as outstanding than what was actually the case. The amount of outstandings continued to grow overtime i.e. the true outstandings were increased by the amount of money stolen overtime.

Motivation	Opportunity	Suitable Target	Fraud Indicator	Fraud Method	Fraud Consequence
Gambling	Lack of segregation of duties concerning the receiving of money, entering into the accounting system and banking	Accounts Receivable	Known to gamble and drink heavily	Taking cash and falsifying bank deposits	Deficit in the amount banked and that received at the bank Increase in the amount of "outstandings" overtime which equated to the amount stolen

Case 3: Dan

The employee was a project manager who awarded contracts to a sub contractor in return for secret commissions. The employee corrupted the tendering process by including a false tender in the contract proposal. This false tender were at rates significantly higher than the employee's preferred sub contractor. The employee had awarded a number of contracts to the

preferred sub contractor all of which were found to be at a rate higher than would be expected within normal commercial terms. The employee's organization were about to undertake a major project to be managed by the employee, the sub contractor would have secured this work which would have meant the organization paid in excess of \$2m more than was consistent with reasonable commercial terms.

Upon investigation of the matter it was found that on all projects in which the employee used the subcontractor that the projects tended to run over budget. It was also found that invoices from the sub contractor tended to be paid earlier than was normal under the organizations operating procedures.

It was discovered during the inquiry that the employee had whilst employed by the organization been a shareholder in a company owned by the sub contractor. This shareholding had ceased a number of years prior to the awarding of the tenders. It was suspected however that the employee still had some interest in the sub contractor's business.

A number of commission payments were made to the employee by the sub contractor. When questioned on this the employee stated that he had done some consulting work for the sub contractor. The total amount of the payments was \$100k. Neither the employee nor the sub contractor were able to provide any credible information evidence of the work alleged to have been performed.

Motivation	Opportunity	Suitable Target	Fraud Indicator	Fraud Method	Fraud Consequence
Revenge/ greed	Lack of scrutiny of the tendering process Lack of segregation of duties in relation to the awarding of contracts	Construction Projects	Close personal relationship with sub contractor	Prepared a false competing tender document of a company which did not exist	Projects ran over budget Early payment of creditor

These cases provide support for the development of fraud profiles and using these fraud profiles to identify the potential for fraud or existing fraud within an organization.

Particular industries are more susceptible to fraud than others. Professional experience in fraud investigation suggests that all industry types are vulnerable, but that certain types of fraud are more common in industries such as construction and insurance. Here, the former is vulnerable to secret commissions, inventory theft and corruption of the tendering process; and the latter is open to claim manipulation or deceit.

The actual act of fraud, however, reveals a pattern of similar methods of perpetration. These include the manipulation of payroll (where ghost employees are paid for services), deceit about accounts payable (where employees authorize payment to themselves or companies they have created), and manipulating accounts receivable (where bank reconciliation statements are falsified).

The Analysis Led Fraud Assessment (ALFA)

Management needs to be aware of and manage the components of the fraud profiles that can manifest. At the very least, it is incumbent upon senior management to recognize a proactive approach as an important part of their responsibility, in attending to organizational and system vulnerability and managing risk accordingly.

One technique this paper offers is analysis led fraud assessment. The methodology is both flexible and focused in assisting management to identify critical areas of fraud risk and assume their responsibility to proactively manage risk. Fundamental to the methodology is the use of the fraud profiles in determining high areas of fraud vulnerability and again through the analysis process in identifying critical areas of fraud risk or indeed fraudulent activity.

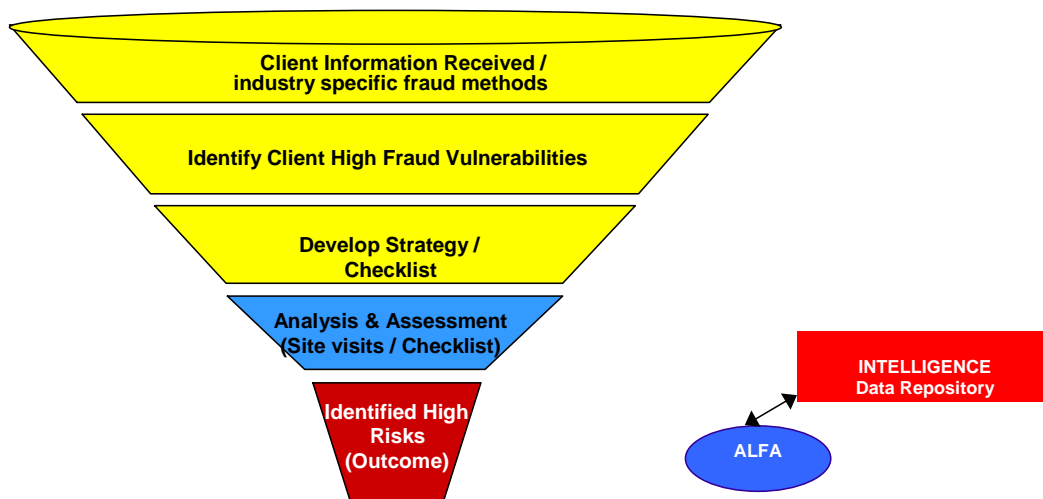
The data for analysis in ALFA is derived from client requested information from within the organisation as well as fraud intelligence data repositories. The organisation is requested to extract any knowledge of previous fraud incidents and any historically relevant information such as previously identified internal control breaches which may give rise to the potential of fraud. The intelligence data repositories include each component of the fraud profiles.

ALFA proceeds through five stages as follows:

1. The receipt of information from the client. Information from an audit. Information from industry specific fraud knowledge repositories.
2. Analysis, assessment and identification of client high fraud vulnerability areas using the fraud profiles and the information gathered in stage one.
3. The development of methodology to investigate these areas.
4. Analysis and assessment of findings and identification of critical fraud vulnerability areas again using the fraud profiles and information gathered.
5. Strategies to identify if fraud is occurring through proactive investigation using the components of the fraud profiles in particular fraud impact/consequence and fraud methods

Each stage is tailored specifically to the industry and organisation. The ALFA process is outlined in Figure 2.

Figure 2 Staged ALFA Process



The ALFA approach brings coherency and flexibility to the fraud prevention process, in identifying areas of high fraud risk, critical fraud risk and potential fraudulent behaviour. A critical risk is defined as an area of high fraud risk where there are poor risk control strategies in place or documented risk management procedures are not being followed.

Once the analysis is completed, a strategy is agreed. Such a strategy may include site visits and data analysis. If it is determined that fraud is being carried out, investigation can proceed. If it is concluded fraud is not occurring, advice is provided to reduce risk and sharpen control procedures.

ALFA has been used both in Australia and overseas, and has identified high-level fraud risks and suspect fraudulent behaviour within organizations. Under normal business conditions, such behaviour and risk is overlooked. The reasons for this abound in business research, and range from the pressures of time, operational complexity, and poor managerial controls. ALFA assignments have included organisations with operations on one site as well as multi-site operations. One recent example included an ALFA review of an organization spread across Australia, England, Ireland, United States, Canada and South Africa, where fraud experts were coordinated in an investigation.

Discussion and Conclusion

These cases are qualitative data that together provide a means to analyse the key elements of fraud – motivation, opportunity and target. Analysis provides an ability to identify and define fraud and ascertain its risk to organizations.

The investigation of crime can be generally categorized as reactive or proactive. While recognizing that prudence would refrain from dichotomies, it is a useful analytical device. Reactive crime management, responds to the crime once committed, such as murder or fraud. Its policing is generally reliant upon one section of law enforcement – detectives. Proactive crime management is driven by intelligence, and involves a broader range of stakeholders in law enforcement – intelligence, detectives, community. Such intelligence is concerned not only with the methodologies for committing crime (that is, how it is done), but also the evidence likely to manifest if such crimes were being committed (that is, spending beyond means, out-of-character displays of wealth). This proactive approach to crime management can be applied to the investigation of potential fraudulent activity. The cases reveal a microcosm of the methods and the evidence of fraud activity. What the Alfa approach suggests is a risk management strategy that is focused, flexible and cost effective to management. It allows management to be a key player in assuming responsibility for managing risk, and utilizing mechanisms and investigative tools that build upon fraud trends and types. If risk is proven, then management can be proactive in its prevention and removal.

Reading

Association of Certified Fraud Examiners (2002) “Report to the Nation on Occupational Fraud and Abuse” <http://www.cfenet.com/pdfs/2002RttN.pdf>

Australian Institute of Criminology (2003) “Australian Crime 2002” <http://www.aic.gov.au/publications/facts/2003/index.html>

Braithwaite, J. (1989) “Criminological Theory and Organizational Crime” *Justice Quarterly*, 6(3):187-209.

Ernst & Young. 2003. *Fraud – The Unmanged Risk*, Eighth Global Survey, http://www.ey.com/GLOBAL/content.nsf/South_Africa/Forensic_Services_-_Fraud_Survey

Graycar, A. (2000) “Fraud Prevention and Control in Australia” Paper presented at the Fraud Prevention and Control Conference, Surfers Paradise, 24-25 August.