CPE 13:

Fraud Prevention

and

Applicable Legislation

THE PRESENTER:

Jonathan Le Roux, a risk management and forensic services professional for over the last ten (10) years, holds a National Diploma in Internal Auditing; has conducted fraud investigations and has attended amongst others an interviewing and interrogation skills course.

Jonathan's experience extends to the Financial, Banking and Private Sector where primary focus was on proactive fraud risk management approaches and strategies to prevent and detect fraud from occurring. Within these areas, Jonathan spent time with both Management and Staff in understanding the causes that lead to fraud as well as what contributes to a successful anti-fraud awareness program.

Ultimately, the time spent with Management and Staff resulted in an improved sense of honesty and integrity; highlighting the importance of culture within the organization and how management (directly or indirectly) can and do change the staff's attitude and behaviour to being ethical whilst employed; greater focus on the approach to take when addressing those high fraud risks within a specified timeframe; the need for an ethical climate and understanding of the roles that both Management and Staff within a company can contribute to preventing and detecting fraud from occurring.

These results have created a sustainable program that can become part of that respective company's corporate governance strategy, in terms of risk management. Often management focuses on the 'bottom-line' issues, whilst neglecting to detect the underlying matters close to the heart of personnel like values, recognition and reward. If these issues are ignored, you will do so at your peril.

Chance favours the prepared mind, Jonathan gets you prepared!

LEGEND:

A. INTRODUCTION 4
Some of the facts 8
Report to the Nation on Occupational Fraud and Abuse 9
B. CORPORATE GOVERNANCE 14
C. CORRUPTION 26
The TI Corruption Perceptions Index 27
The Myth Of Culture 28
CONFLICTS OF INTEREST 31
BRIBERY 33
ILLEGAL GRATUITIES 38
ECONOMIC EXTORTION 38
D. ASSET MISAPPROPRIATION 41
INVENTORY AND ALL OTHER ASSETS 41
CASH THEFT SCHEMES 42
REGISTER DISBURSEMENTS 43
EXPENSE REIMBURSEMENT SCHEMES 44
BILLING SCHEMES 45
PAYROLL SCHEMES 46
CHEQUE TAMPERING 46
E. FRAUDULENT FINANCIAL STATEMENTS 48
TIMING DIFFERENCES 51
FICTITIOUS REVENUES 52
CONCEALED LIABILITIES AND EXPENSES 53
IMPROPER ASSET VALUATION 54
IMPROPER DISCLOSURES 55
The fundamental differences between fraudulent financial reporting *and the* misappropriation of assets: 56
H. COMPUTER CRIME – THE NEW THREAT 64
Selective Computer Crime Timeline 68
I. REDUCING YOUR FRAUD RISK – Prevention 70
FRAUD HEALTH 'CHECK-UPS' 70
FRAUD PREVENTION: A FOUR-STEP APPROACH 72
J. REDUCING FRAUD RISKS AT STAFF LEVEL 75
FRAUD PRONE PERSONALITY TYPES 75
THE FRAUD TRIANGLE 77
ETHICS 82
COMPILING A FRAUD PREVENTION AND DETECTION PLAN 85
K. CONDUCTING FRAUD AWARENESS PROGRAMS 86
LEARN FROM OTHER'S MISTAKES – LESSONS FROM LEESON 88
L. FRAUD DETECTION 89
"RED FLAGS" OF MANAGEMENT AND CORPORATE FRAUD 89
Using CAATTS to detect fraud 91
Benford's Law 93
FRAUD HOTLINES 93
PROACTIVE FRAUD AUDITING: A FIVE-STEP APPROACH 96
FRAUD INVESTIGATION 98
THE FRAUD RESPONSE PLAN 99
M. APPLICABLE LEGISLATION 100
N. CONCLUSION 104
Frequently Asked Questions 106
STATISTIC & ARTICLE SOURCES 111
ANNEXURES 112

A. INTRODUCTION

In the managing of a business, irrespective of its size, one needs to consider the risks associated with the running of that business coupled with the means to address and/or combat those risks effectively. In the assessment of these risks, one needs to be aware of the exposures that may be prevalent to that business both internally and externally.

When a business is started or is growing at a rapid rate, we are often focused on the core service or skills that we bring to the table. Our focus is not so much on the running of the business, but more on the delivery of the service. It is often in times like these – in growth stages of our business – that we can be exposed to elements that we are not prepared for, like fraud.

What is critical for businesses to know is that fraud is a business risk and the management thereof is of utmost important for any sized business. There may be many risks that pose a serious threat to the 'health' of a business, but fraud is a real threat – a threat to the financial well-being of a business and to its image and reputation.

Although we like to think of fraud as something that happens to other people, it is an unwelcome fact that all organizations (small, medium or large) are potential victims. Fraud is now one of the major causes of business failure.

In a Fraud Advisory Panel Guide, mention is made of a survey conducted by the ACCA in 2001 that indicates that **75% of frauds in smaller businesses were committed by owner-managers themselves**; 20% were committed by employees; 2% were committed by owner-managers colluding with employees; and a further 1% were committed by employees colluding with third parties.

So, the threat of fraud does not always stem from outside the business, most frauds are the subject of internal workings, which could prove disastrous and even closure of the business. Fraud involves deliberate deception that can remain undiscovered for years and is committed by people in all walks of life. Employees, owners, directors and international crime syndicates are all potential white-collar criminals.

"Fraud and deceit, abound in these days more than in former times"
- Sir Edward Coke. Lord Chief Justice (1602)

Fraud is among the oldest human occupations. Ever since Jacob obtained Isaac's (his father's) blessing by impersonating his brother Esau, the effort to get something for nothing has been a recurring theme in Western literature and law. This oldest story of fraud is told in Genesis 27. Today, Jacob and his mother, Rebekah, could have been charged with fraud and conspiracy.

Some of the business views expressed are that the fraud amounts are small and are therefore of no significant concern or risk to the business. This is an unsettling view as fraud is something that grows more rapidly over time and although the value or risk NOW might seem insignificant or small, it does grow exponentially and will destroy a business – maybe not yours, but somebody else's!!

Small frauds should be important to every insurer, every business that is self-insured or uninsured, all businesses with large deductibles or self-insured retentions and any business who deals with the public. ***The wise fraud perpetrator knows that insurers, businesses and police have inadequate resources to fight small frauds***. Criminals tend to gravitate to the crime with the least chance of

prosecution and the greatest chance of profit. ***The small fraud is the crime of choice*** for those attempting fraud and insurers and small businesses are hurt most. It is often where retailers and restaurateurs lose money regularly.

For the SMME business segment, the most common types of fraud are the ones that **impact on the profit and loss account** as a result of overstating expenses or understating income. Although the individual amounts may be relatively small, they are not easy to detect. Many fraud indicators within the SMME business may go undetected or unnoticed (changes in cash flow patterns, variations in accounting ratios, stock shrinkage, customer complaints, etc) but they do place an SMME business in a vulnerable state during a growth or rapid expansion phase of their business.

Frauds are most effective in amounts ranging from R40 to R4000. The volume of small frauds is great. They are not exciting to investigate. Small frauds do not seem to be worth the bother of a Certified Fraud Examiner or other authority. ***Small frauds are to business as a mosquito bite is to a bull elephant***. However, I must caution you, if that mosquito carries a disease, it can kill the elephant. The mosquito of the small fraud has made some industries ill, it remains to be seen if the disease is fatal.

So what's the cure? What preventative medicine can we provide to the ailing industry? Zero tolerance for fraud; an anti-fraud culture; code of ethics; prevention and detection strategies, are but some means to solve these mosquito bites.

Fraud is compared to death by a thousand cuts; it inflicts pain and does result in a loss of blood (profits), although only a slow trickle is seen, the result is the same, potential business closure.

In South Africa fraud is defined as:

"The unlawful and intentional making of a misrepresentation which causes actual prejudice, or which is potentially prejudicial to another."

Therefore, Fraud comprises the following elements:

- **Unlawfulness**
  – the action must be seen to be wrong in the eyes of society

- **Misrepresentation**
  – a false statement made by one person to another
  – the misrepresentation may take the form of words; words & conduct; or just conduct
  – a misrepresentation may also be a failure to disclose certain information in circumstances where there is a duty to do so.

- **Intent**
  – the person making the misrepresentation must have intended, or foreseen that the victim would be deceived.

- **Prejudice**
  – the victim would have suffered prejudice by reason of altering his position to his detriment after

relying upon the misrepresentation. Potential prejudice is also sufficient if it is reasonably possible that the victim, relying on the misrepresentation, would have suffered harm.

It is important to remember that white-collar fraudsters do not act like gangsters - they are charming, respectable people, able to seduce colleagues into believing in their integrity. They are often long-serving and trusted employees, and the very last people one would suspect. (From the last two international fraud surveys conducted by Ernst & Young and KPMG, it was found that approximately 80% of all frauds involved employees)!

The risk of becoming a victim of major financial fraud is increasing, so it is imperative to create systems that defend against these risks. To quote Business Against Crime, ***"100% of all businesses in South Africa are affected by commercial crime. It is only the extent of this crime that differs from company to company".***

Fraud is now being called the 'crime of choice' for the new millennium. It is a fact that in white-collar crime the potential rewards are much greater than in blue-collar crime, the risk of detection is lower, successful prosecution is more difficult, and the penalties are less severe. These are all sound 'business' reasons for both small-time criminals and international crime syndicates to put their efforts into fraud, and our extent of preparedness for this growing challenge needs to be continuously monitored and assessed if we are to cope with the problem.

Fraud and the existence thereof are more prevalent during growth phases of business, thereby creating other opportunities due to the following:

- Where businesses are growing or expanding, greater risk is attracted – this could be due to the owners/managers not being good at core functions and having to rely on others for non-core competencies like accounting support, HR management and keeping abreast of IT changes (systems developments, virus detection).
- Key functions are being outsourced - These outsource functions may include the IT environment (or parts thereof) the Accounting function (or parts thereof), Human Resources (depending on size of business) and other industry-specific professional services
- DTP (Desk Top Publishing) means that the difficult is made simpler due to the ease at which one can produce fraudulent invoices, bank statements and any other documents that is needed to authenticate a transaction – another reason why the control function is critical.
- The mobile workforce is becoming acutely aware of technology, trends and tricks to 'engineer' themselves to become more successful - more able to override internal controls.
- Businesses that are on a pruning drive to cut costs may do so at the peril of the business, often removing key controls and resulting in less people in management with even lesser checks.

It would seem that the issue of how to combat fraud continues to occupy pride of place at many conferences, but perhaps not so within many businesses. We continue to hear a lot of talk about the problems but we are not seeing much action. Hence this training course is designed to help you learn more about fraud prevention and the applicable legislation. We believe that this workbook should be used as the catalyst to question the effectiveness of fraud risk management in both your business and the clients that you serve.

For any business wishing to reduce the risk of being a victim of commercial crime, it is imperative that a coherent strategy be developed to address the various risks. An effective fraud deterrence strategy comprises of at least the following four phases:

- **Phase 1** – an *understanding and assessment of the risks* facing your business. This will include an internal audit of your existing controls and an external analysis of your existing documents to see if there are any "Achilles' heels" that the criminal could exploit.

- **Phase 2** – the *implementation of solid prevention techniques and procedures* – this would include upgrading internal controls, printing new custom cheques that contain effective and appropriate security features, as well as the compilation of a fraud prevention and detection plan. Basically plugging all the gaps found in phase 1.

- **Phase 3** – *fraud training*. This would encompass regular (technical and general awareness) reinforcement training for all relevant staff.

- **Phase 4** – *appropriate reaction planning*. This would be the compilation of a fraud response plan, because no method of security can offer 100% protection and your staff need to be alert to this fact and know how to react should a fraud be detected.

Though no method of security can offer complete protection, criminals would be more likely to take the path of least resistance. Compare effective security features to your home security. A house with a high-tech burglar alarm, electrified fence and an Alsatian or two is less likely to be burglarised than a similar house with less, or even no, security. The criminal is then encouraged to move on to the easier target.

Fraud prevention is like running a race with no finishing line. As the criminal becomes more sophisticated in his/her attempts to steal our money, so must the effort to create better security features increase, thereby slowing fraud proliferation. That is why it is critical for you to become a business that keeps abreast of the latest in occupational fraud and who is applying the correct technology and taking ordinary care, thereby ensuring that the risks from fraud, and the liability for loss, can be considerably reduced.

In designing your businesses fraud strategy keep in mind that the ideal in fraud prevention, i.e. 100% checking, is not cost-effective, and that financial criteria will need to be set.

Businesses happily devote large quantities of resources to re-engineering business operations to achieve modest gains in productivity.
How much is being devoted in your business to control fraud?

Some of the facts

The most obvious object of fraud is the cheque and the computer, and many statistics, newspaper headlines and Crime Report ratios paint the picture of opportunistic criminals and unenlightened businesses:

- 80% of most fraud involves **employees** – either working alone in collusion with third parties. U.S. employees steal about $120 billion annually, with the average computer crime netting $250 000, and the average cheque fraud garnering $125 000 compared with $4 000 for the average bank robbery;

- It is estimated that less than 13% of fraud losses - worldwide - are ever recovered;

- Cheque fraud is estimated to be growing by 12 – 15% annually while the FBI estimates that computer crimes are growing by between 200 – 500% per annum;

- Crimes of fraud and forgery are prevalent, difficult to investigate and usually go unreported. Because of this, no one really knows the full picture;

- In some cases, fraudulent cheques are not investigated unless they exceed R1 000 000-00 in value and computer frauds are not investigated unless they exceed R28 000 000-00 in value;

- Breaking into networks is quite common in the commercial sector, but industry does its best to keep it quiet – in his book 'computer security', J. Carroll states that ***"computer crime may be the subject of the biggest cover-up since Watergate";***

- There are an estimated 200 known organised crime syndicates currently in S.A.;

- The World Economic Forum says that S.A. has an organised crime problem second only to Colombia and Russia;

- ***"We are not at risk",*** and ***"It has never happened to us",*** are extremely dangerous and possibly expensive attitudes to have;

- ***Fraud may be consuming an average of 6% of your gross turnover;***

- The number of frauds is expected to grow, and the S.A. criminal justice system is not equipped to deal with this increase, so the private sector is going to have to take up the slack, with the preventative effort starting with **YOU** and the skeptical auditor.

Report to the Nation on Occupational Fraud and Abuse

The Association of Certified Fraud Examiners (ACFE) is the recognized authoritative source for all types of information about fraud and white-collar crime. The Association's 'Report to the Nation on Occupational Fraud and Abuse' (1996, 2002, & 2004) is the first study of its kind. This is not a random survey - the data presented in this Report is based solely on 2,608 cases, the biggest of which involves $2.5 billion. As a general rule, only more serious fraud and abuses are included. The Report is the largest known privately funded study on the subject.

The Report to the Nation on Occupational Fraud and Abuse has four goals...

- Summarize the opinion of experts on the percentage and amount of organizational revenue lost to all forms of occupational fraud and abuse
- Examine the characteristics of the employees who commit occupational fraud and abuse
- Determine what kinds of organizations are victims of occupational fraud and abuse
- Categorize the ways in which serious fraud and abuse occurs

The following statistics about fraud & white-collar crime are from the ACFE's Report:

- Fraud and abuse costs U.S. organizations more than $400 billion annually.
- The average organization loses more than $9 per day per employee to fraud and abuse.
- The average organization loses about 6% of its total annual revenue to fraud and abuse committed by its own employees.
- The median loss caused by males is about $185,000; by females, about $48,000.
- The typical perpetrator is a college-educated white male.
- Men commit nearly 75% of the offenses.
- ***Losses caused by managers are four times those caused by employees.***
- Median losses caused by executives are 16 times those of their employees.
- ***The most costly abuses occur in organizations with less than 100 employees.***
- The education industry experiences the lowest median losses.
- The highest median losses occur in the real estate financing sector.
- Occupational fraud and abuses fall into three main categories: asset misappropriation, fraudulent statements, and bribery & corruption.

The Report classifies the numerous methodologies used by employees to commit occupational fraud and abuse, which can be divided into three broad categories:

Corruption (constituted 10% of offenses): Black's Law Dictionary defines corruption as "the act of an official or fiduciary person who unlawfully and wrongfully uses his station or character to procure some benefit for himself or for another person, contrary to duty and the rights of others." Corruption, in the sense of occupational fraud, usually involves an executive, manager, or employee of the organization in collusion with an outsider. There are four principal types of corruption: bribery, illegal gratuities, conflicts of interest, and economic extortion.

Case Study #2019:
A married buyer for one company convinced his superiors that business supplies purchased from 3 particular vendors were the best on the market. But the buyer's judgment was clouded by the fact that these vendors together had paid him $250,000 in kickbacks to buy their goods.

Case Study #1440:
A 48-year-old manager was very partial to one of his company's outside consultants. The manager ultimately suggested that the consultant, in addition to his regular billing, submit occasional fictitious bills to the company. The manager would then approve them for payment. Together the twosome split $300,000 of the company's money.

Case Study #15:
The purchasing manager and another employee cost a manufacturing company $2.8 million. They conspired with one of the company's suppliers to send bills to the company for products never delivered. The manager and his employee would approve the fake invoices for payment.

Asset Misappropriation (which accounted for 85% of offenses): Asset misappropriation was by far the most common form of occupational fraud, constituting more than four out of five reported offenses. Assets are misappropriated either directly or indirectly for the employee's benefit. Although any tangible asset can be misappropriated, certain assets are more susceptible than others are. Transactions involving the organization's cash and checking accounts were far more common than all other asset misappropriations combined. Other susceptible assets include inventory, supplies, equipment, and information.

Case Study #98:
The 67-year-old owner of a savings and loan association diverted millions of dollars in corporate funds to cover his own bad investments. The final cost of the fraud to taxpayers was $2.5 billion.

Case Study #1842:
The director of taxation for a large company, who had a post-graduate degree, conspired with a partner of one of the company's "Big Five" auditors. Together they set up a shell company controlled by the director's wife. They paid the shell $1 million in bogus billings over 3 years.

Case Study #1401:
A male bookkeeping employee of one company knew how busy the boss was at certain times. The employee always presented a stack of checks for the boss' signature during one of those busy times. The employee regularly slipped in an extra check for himself, which the boss would sign in haste. This oversight cost the company $150,000.

Case Study #1090:
The accounts payable supervisor for a 5,000-employee oil company embezzled $639,000. He established his own outside company and approved fake invoices for his phony operation.

Case Study #1515:
A bookkeeper in a four-person legal office wrote 22 checks to herself and forged a partner's signature, eventually stealing $186,000. Her fraud was discovered shortly after she resigned. The law partner later learned that she had two prior embezzlement convictions and had served four years in prison before coming to work for him. After she resigned from the law office, she went on to steal from two more employers.

Case Study #1747:
A 55-year-old MBA recipient was an avid biker. So avid, in fact, that he charged a $5,000 mountain bike to his company as "construction equipment." He was caught when he tried to claim reimbursement for an out-of-state biking convention. The executive had falsely described his trip as a "management seminar."

Case Study #1819:
A degreed male, 32, started a software company using his employer's time, equipment, and facilities. His employer, also a software company owner, discovered that the employee even demonstrated his own products to the company's customers. Ultimately, the employee diverted $500,000 in business away from his employer.

Case Study #2389:
A university graduate and government employee once used her government credit card for personal purchases in an emergency. When no one detected her action, the employee charged another $4,500 in personal items to the government.

Fraudulent Statements (accounted for 5% of offenses): Fraudulent statements are the third broad category of occupational fraud. These statements, in order to meet the definition of occupational fraud, must bring direct or indirect financial benefit to the employee or his/her organisation. Although all fraud involves "fraudulent statements," this category is limited to two sub-categories: fraudulent financial statements (which is committed for the benefit of the organisation) and all others.

Case Study #1932:
Six directors of a family-owned electronics company pocketed more than $100 million by selling overvalued company stock. The company's earnings and profits had been significantly overstated through false financial statements prepared by the family members.

Case Study #1711:
The acting director of admissions for a university knew his job was only temporary. To enhance his CV, he created the necessary fake transcripts to "award" himself a degree.

Occupational fraud and abuse encompasses a wide variety of conduct by employees, managers, and directors of organizations ranging from pilferage to sophisticated investment swindles. Common violations include asset misappropriation, corruption, false statements, false overtime, petty theft and pilferage, use of company property for personal benefit, and payroll and sick time abuses. The key is that the activity...

- Is clandestine
- Violates the employee's fiduciary duties to the organization
- Is committed for the purpose of direct or indirect financial benefit to the employee
- Costs the employing organization assets, revenues, or reserves

REPORT CONCLUSIONS:

1. Certified Fraud Examiners consider the problem of occupational fraud and abuse to be a serious one. CFEs generally occupy positions within organizations where they investigate a wide range of abusive and fraudulent behaviour. ***They are aware not only of the direct costs of the behaviour, but also of the indirect costs: loss of productivity, pilferage, and related expenses.***

2. There is a direct correlation between the employee's age, sex, position, and the median loss due to fraud and abuse. The data revealed that the ***most predictive variable concerning the amount lost was the perpetrator's position in the organization***. As a general rule, men and older employees occupy higher positions and therefore have greater access to assets.

3. ***Smaller organizations are the most vulnerable*** to occupational fraud and abuse. Organizations with 100 or fewer employees suffered the largest median losses per capita. Generally, this is because sophisticated internal controls, designed to deter occupational fraud, are less prevalent in smaller organizations.

4. ***A lack of understanding of the nature of occupational fraud and abuse adds to its cost.*** Certified Fraud Examiners frequently comment that executives often are reluctant to believe fraud and abuse occurs within their organizations. Because of their clandestine nature, many of these offenses go undetected until significant losses are incurred.

5. Relatively few occupational fraud and abuse offenses are discovered through routine audits. ***Most fraud is uncovered as a result of tips and complaints*** from other employees. To deter and detect fraud and abuse, many experts believe an employee hotline is the single most cost-effective measure. Some organizations install their own hot lines, while others use a subscription service.

6. ***The expansion of computers in organizations will likely increase losses due to occupational fraud and abuse***. The use of computers in business has drastically changed the speed with which financial transactions can be accomplished. In addition, computers often do not create the documents necessary to easily detect fraud and abuse. Many experts see increasing reliance on computers as a likely cause of additional offenses. However, computers are also being employed to detect fraud and abuse.

7. ***The rate of occupational fraud and abuse likely will rise***. It is caused by many complex sociological factors. Individual and corporate moralities are difficult to quantify. Among other things, increasing demands on the criminal justice system by violent criminals may make fraud and abuse prosecutions more difficult. Additional proactive vigilance and education, however, as well as consumer action, could stem future increases in occupational fraud and abuse.

A short glossary of fraud terms:

Bribery: where an official accepts money or some other consideration to engage in a particular course of action, or inaction. Official (government employee or elected official) bribery involves a promise for acting or withholding some official act. Official bribery *(Corruption)* is unlawful in most cultures. *Commercial Bribery* is known as "facilitating payments" in some cultures and is not a crime in most cultures, although it often is against the organization's policies and procedures.

Conflict of interest: where an employee/official stands to profit incidentally from an act. This could involve a planning decision that has the effect of increasing the value of property owned by the employee, or the awarding of a contract to a company in which the employee has a financial interest.

Corruption: An employee's exploitation of his/her position for personal gain.

Embezzlement: Theft of money, under that employee's control, from an employer by an employee using false entries in accounting records to cover up the crime. An embezzler is typically an accountant, bookkeeper or manager who is able to divert income and then cover it up.

Extortion: where an employee/official demands money or some other consideration to engage in a particular course of action, or inaction.

Fraudulent financial statements: Directors and/or managers falsify financial statements in order to deceive investors, the public, creditors, banks or other lenders.

Fraudulent non-financial statements: Employees falsify employment credentials or internal/external documents like invoices and expense claims.

Kickback: A payment by a vendor to an employee at the request of the employee in order for the vendor to receive favourable treatment.

Lapping: Stealing a customer payment and then using a subsequent customer payment to cover the previous customer's account. These overlapping payments create a "float" of money that can be used as long as all payments are eventually posted. What usually occurs is that the lapping process builds up like a giant pyramid until it falls apart when not enough payments are available to cover the amounts owed.

Larceny: Stealing cash or assets that have already appeared on the company's books.

Skimming: Stealing cash or assets before they have been entered into an accounting system.

Theft: The unlawful act of taking property without the owner's consent.

B. CORPORATE GOVERNANCE

The main aim of this section is to give everyone a better understanding of what is included in the King Report on Corporate Governance for South Africa 2002, to give it its full title, or King II for short.

DEFINITION OF CORPORATE GOVERNANCE

Firstly a definition to help clarify what corporate governance is as many people still struggle with the concept. This is one of many in existence and expands on the one Cadbury used in the early 1990's, which simply stated that corporate governance is **"the system by which companies are directed and controlled"**.

A GLOBAL PERSPECTIVE

Corporate Governance has been a global issue since the early 1990's after a series of financial scandals in the late 1980's and early 1990's. Attention was focused on the role of Directors in managing corporate affairs, and in particular, on the operation of internal controls over the financial aspects of a business. As a result the Cadbury Report in the UK and the Treadway report in the USA were commissioned.

South Africa followed suit soon after and the King Report was published in 1994. It addressed similar areas as Cadbury and Treadway, but also included a Code of Ethical Practice for business enterprises in South Africa.

The Greenbury Report in the UK was commissioned in response to the growing demand for greater disclosure and transparency of Director's remuneration, following a series of "fat cat" pay rises. South Africa did not have an equivalent, until recent JSE listing rules require individual remuneration disclosure for directors and now King II.

Hampel relooked at all the codes and practices and ultimately came up with the Combined Code, which is an attempt to consolidate the earlier developments in Corporate Governance. The London Stock Exchange required disclosure on how certain principles were being applied, and whether or not the provisions were complied with throughout the accounting period.

The Turnbull Report was commissioned at the request of the London Stock Exchange who wanted further guidance on one of the principles contained in the Combined Code, namely around risk management and internal control.

The Blue Ribbon Report from the US focus's on Audit Committee's.

In South Africa it was decided to re-look at the King report and update based on the global developments in corporate governance, the practicalities of applying the codes and the changing economic environment in South Africa.

GENERAL POINTS FROM KING II

- ***Accountability*** is at common law and statute to the company if one is a director; not accountable to everyone. Responsible to stakeholders that have been identified as relevant.
- ***Inclusive approach*** – recognises that stakeholders such as the community, its customers, employees and suppliers need to be considered. Courts have rejected the shareowner dominant theory – which shareowners are entitled to expect directors to run the company in their sole interests – in various jurisdictions, because on incorporation a company becomes a separate legal persona and hence cannot be owned. Shareowners have a right to vote and a right to receive dividends, but they change whereas the company remains constant. Consequently directors must act in the interest of the company, which in turn needs to take account of all stakeholders.
- ***Performance*** – refers to enterprise/risk taking/business decisions. This is an integral part of what drives a business.
- ***Conformance*** – constraints of shareowners expectations of capital growth and responsibility to various stakeholders.
  – Sloth: loss of flair when enterprise gives way to administration.
  – Greed: directors make short-term decisions because of impact on, eg, share options etc.
  – Fear: directors become subservient to investors.
- ***New Legislation***, e.g., Labour Relations Act, Basic Conditions of Employment Act, Employment Equity Act, National Environmental Act, Insider Trading Act, Public Finance and Management Act, Banks Act. Also, JSE Listing Requirements revised in 1995 and 2000. Companies Act revised around liability insure disclosure of beneficial owners of shares held by nominees, company secretary mandatory.
- ***IT*** – has become a key driver of business strategy and decision. The increase of cheap, accessible communication via the Internet has had a major impact on the internal controls. Therefore, the right skills have become and will continue to be a major issue.
- South Africa ranked in the top 5 of 25 emerging markets, due to poor disclosure and transparency, yet King I was considered one of the best codes of its time and King II, is already recognised as the most comprehensive work. ***We have great theory, but poor practice***. Attitudes must change if we are to get investors coming into the country and be able to compete in the global community. Minimalist compliance and disclosure etc will lead to capital leaving the country.
- ***Triple bottom line reporting*** endorsed:
  - economic: financial and non-financial aspects
  - environmental: effect of products and services on environment
  - social: values, ethics and reciprocal relationship with stakeholders
  - It is generally accepted that “demonstrating concern creates an atmosphere of trust and a better understanding of corporate aims, so that when the next crisis comes (and these are inevitable for big companies) there will be a greater goodwill to help the company survive.”
- ***Reputation Assurance***.

SEVEN PRIMARY PRINCIPLES OF GOOD CORPORATE GOVERNANCE

- **Discipline** – correct and proper behaviour of senior management.
- **Transparency** –ease with which an outsider is able to make meaningful analysis of a company's actions, its economic fundamentals and non-financial aspects
- **Independence** – minimise or avoid potential conflicts, for instance dominance of CEO or large shareowner.
- **Accountability** – of decision makers for decisions and actions. Mechanism must exist for this, for queries and assessment.
- **Responsibility** – allows for corrective action and penalising of management.
- **Fairness** – balanced in taking into account all those who have an interest in the company and its future.
- **Social Responsibility** – aware of and respond to issues, placing high priority on ethical standards: non-discriminatory, non-explorative, and responsible to environment and human rights.

COMPLIANCE AND APPLICATION

- The Report and its resulting code is not embodied by any law and is ***considered to be best practice and hence self regulatory.***
- It does however recommend who should adopt the code, which has been extended from King 1, to include: all companies on the JSE; banks, financial and insurance entities as defined in the various legislation regulating the SA ***financial services sector***; ***public sector*** enterprises and agencies that fall under the PFMA and Local Government: Municipal Finance Management Bill. It is also recommended as best practice for private companies.
- The JSE have confirmed that they will update their listing requirements to cover King II.
- The committee believes peer pressure and shareholder activism will encourage people to comply and that the findings of the various McKinsey surveys – that shareholders will pay a premium of between 18-27% for companies with good governance – will act as a carrot rather than a stick.
- For all financial years commencing 1 March 2002.

THE CODE OF CORPORATE PRACTICES AND CONDUCT

- As with King I, the entire report is approximately 300 pages long, but this is summarised into The Code of Corporate Practices and Conduct. This is split into the eight sections, with Risk Management and Integrated Sustainability Reporting being the two major new areas.
- The new code is much larger than the old one, with approximately 130 separate principles or paragraphs where as the old one were just over 30.

PUTTING KING II INTO FOCUS

Here we attempt to take the principles and guidance from King II, particularly around risk management, internal controls and internal and external audit, and put them into a practical and continual process.

The four central parts are the fundamentals of any risk framework:

- **Shareholder value based:** the company's risk management system should have a full understanding of the stakeholder requirements as its core and be focused on sustaining the creation of shareholder value.
- **Embedded:** the ***culture of the organisation should reflect the risk consciousness*** of the board. This requires a suitable organisational structure, policies and procedures, and appropriate staff training in risk management which enables risk to be managed at all levels of the business.
- **Supported and Assured:** the system should provide management with the ***assurance it needs that risks are being managed appropriately***. This assurance should go beyond the embedded monitoring procedures, which are also required to be in place.
- **Reviewed:** the board should review the effectiveness of the system of risk management on a regular basis in the light of current business performance and future expectations. This rigorous top down approach should consider its ongoing contribution to the effective and efficient operation of the business.

The process then starts with the setting of the Strategic Objectives of the group, which should be taking account of what drives shareholder value. From this potential risks are identified and evaluated. Responses to the risks are then decided upon and may include:

- Transfer
- Mitigate
- Eliminate
- Reduce
- Accept
- Increase

The internal control framework is part of all these responses and should include both preventative and detective controls as appropriate. The responses are then assigned ownership and expectations are communicated. Management will need to ensure the commitment and capabilities to deliver these responses exist and systems need to be put in place to monitor their operation. Where problems arise corrective action needs to be taken.

Internal audit and external audit are the two "standard or common" assurance providers, but others may include ISO accreditors, health and safety officers etc. Their activity should be coordinated to avoid duplication of effort, where appropriate, and the findings need to be communicated to the correct level and corrective action taken where necessary.

The board must have processes in place to review the overall effectiveness of the system looking for areas of improvement. This process and outputs need to be communicated with stakeholders, traditionally via the Annual Report.

This whole system then starts again.

WHY SHOULD YOUR BUSINESS COMPLY WITH KING II?

Good business sense

Good governance can be seen to contribute to the longevity of the group through better decisions, evaluations, risk identification and agreed responses, improved monitoring process and corrective actions.

Reputation management

Per Reputation Assurance "demonstrating concern creates an atmosphere of trust and a better understanding of corporate aims, so that when the next crisis comes (and these are inevitable for all businesses) there will be a greater goodwill to help the business survive."

Increased shareholder value

These two will contribute to improved and sustainable results for the company and hence increased shareholder value.

WHAT CAN YOU NOW DO TO ENSURE COMPLIANCE WITH KING II?

- A compliance review is an interview-based tool aimed as assessing the current state of the governance structures against and desired future state and best practice, including King II requirements. Director's perceptions on how things work and how they can be improved can vary greatly and maybe certain areas have been "defined" very well but are not in fact working according to that definition. Also, every company will apply the governance principles differently to take account of their specific circumstances. Hence we believe an interview bases assessment it more meaningful than a checklist. It also allows input from ourselves and what is best practice is, i.e., what companies are doing

- An Assurance Report is basically an opinion on the corporate governance disclosures in the Annual Report that confirms that they have substance. This is aimed at companies who want to differentiate themselves in the market place from all the boiler plate wordings that have been prevalent up to now.

- There are various offerings around risk assessment strategies and frameworks that help companies identify their risks and respond to them.

- And finally, there are on offer various internal audit related services, from full outsourcing to assistance with developing a methodology.

KING II & FRAUD

- The King II report urges organisations (both private and public) to adopt **ethical codes** which, if supported by effective communication channels and training, and is seen to be enforced, could contribute to the development of a moral business culture in South Africa.

- A key Corporate Governance responsibility should be to facilitate confidential **whistle-blowing** mechanisms and ensure that justified whistle blowers are not penalised, but praised for their efforts on behalf of the organisation.

- Every business should prepare a **disaster recovery plan** to ensure continuity of its operations in the event of a catastrophe.

- It is essential for every organization to establish systems that **identify risks** early and continuously and then to establish internal controls to mitigate the risks.

EXAMPLES OF CORPORATE GOVERNANCE FAILURES IN SA…

1. **Macmed** *(Financial Mail 22 & 29 October 1999, and Business Day 6 February 2004)*

Macmed was put into **provisional liquidation** at the company request on October 15, 1999. The liquidation stands out for its size and its suddenness. With the total exposure, by more than a dozen banks apparently exceeding R 1bn, it was described as the largest failure in SA corporate history.

The main cause of the failure of the group was due to poor corporate governance particularly in respect to overall management of the affairs specifically financial matters of the group.

Some of the failures included the financial irregularities specifically the operation of the Macmed trust account held by one of the group's former attorneys who was also a director of Macmed but resigned around the beginning of October 1999. The trust account had "very strange payments" which investigators from accounting firm KPMG, who were conducting a forensic investigation into Macmed's affairs, were attempting to unravel. The purpose of the account was not known and huge amounts of money passed through the account.

There was poor administration of the financial affairs of the group which resulted to a huge debt on the company's books and hence its ultimate liquidation.

In February 2004 a Pretoria judge found Macmed Company secretary Alan Hiscock and financial manager Johann Muller liable for the failed company's R647m debts.

This brings to an end the biggest civil trial in South African history.

2. **Specialised Outsourcing** *(Financial Mail 14 July 2000)*

Institutional investors in Specialised Outsourcing plan to sue the group and non-executive directors for what they see as misleading information about its activities.

The founder and ex-CEO, Dave King, sold out of the group without warning the investors. The founder departed from the group in November 1999 and the other shareholders were not adequately informed.

As a result of the above, the share price of the group fell from 2850 cents in January 2000 to 1200 cents in July 2000. This resulted to a situation where Ernst & Young, the newly appointed auditors, were required to review the financials back to 1997.

3. **Siltek** *(MoneyWeb 19 October 2001)*

Company put into liquidation in October 2001 after a capital restructuring plan failed

The share price moved from R 7.50 in February 2000 to 45 Cents in February 2001 while the shares were suspended in October 2001 at a price of 10 cents.

Poor management decisions on management changes and restructuring programmes brought the company down. Specifically: -

- Over-expansion that left the business with excess capacity and unsuitable cost structure.
- A new accounting system for Siltek distribution dynamic implemented in November 1999 resulted to poor operating controls and led to stock losses.
- The problem with the Australian operations that led to its closure in July 2001.
- High Level of Gearing and the interest costs of that debt.

4. New Africa Investments (NAIL) - *Financial Mail 30 April 1999*

Due to the poor corporate governance, *the share price of NAIL became disappointing.*

The issue that eroded the investors confidence and hence resulted to the fall in share price involve the fact that four executive directors proposed to transfer from the company to themselves the 3.7m AMB share options which were not linked to performance and the terms of the options were no transparent. Several questions remained unanswered in regard to this deal, which included; On what basis did remuneration committee of NAIL board approve the transfer? Did the remuneration committee seek advice from legal and remuneration experts on the matter?

As a result of this, in 1999, shareholders ousted two of the controlling executive directors, Nthato Motlana and Jonty Sandler.

5. JCI (Financial Mail 6 February 1998)

The chairman of the company Mzi Khumalo and poor decisions made by individual directors caused the break up of JCI as supported by the following facts: -

(i) Different factions on the board pursuing different strategies which resulted in a chaotic situation in the board

(ii) The Chairman forced the sale of JCI's Gold mines, Western Areas and Joel, to Anglo in return for his long-cherished stake in Lonrho and Cash

(iii) The Chairman made a controversial decision, without board approval, to invest R252m of JCI's money in Southern Mining Corp (SMC). Khumalo had earlier made a personal investment in SMC, a company that wanted to develop a titanium deposit. The deal was however reversed.

(iv) Mr Kebble's decision (a director) to buy Beatrix shares worth R 290m with no board approval

Khumalo resigned after a deal between JCI and Southern Mining - a company in which his family had a minority stake - was struck without board approval.
The share price of JCI fell form 5050c in February 1997 to a low of 1595 in November 1997.

6. **Bryant Technology** *(Financial Mail 4 February 2000)*

The poor performance of the company was aggregated by the poor corporate governance in regard to misrepresentation to the shareholders by the directors – poor communication.

In the case of Bryant Technology, the financial statements for the period to 30.06.1999 had to be restated due to "incorrect accounting procedures" because of "gross management irregularities". The restated position reflected that the previous balances were grossly misstated and was done with aim of making the share speculative to buy.

Financial performance as per the reports issued by directors.

Period	*Turnover R m*	*Operating profit R m*	*Pre-tax profit R m*	*Headline Earnings ©*
28.2.98	9.4	0.6	0.4	0.14
30.6.99 *published*	34.9	8.2	9.4	3.32
30.6.99 *restated*	17.3	(9.2)	(4.4)	(4.32)

In this case, signs of disaster emerged in November, when CEO Richard Bryant abandoned the company he founded in 1973. With him went financial director Nicole Wade. No wonder, judging from a horrific restatement of 1999's results. Making this sordid issue worse is that, on face value, original figures audited by KPMG made the share a speculative buy. Focus was on thin technology acclaimed by the Gartner Group as a major PC networking advance. Shareholders are now told that thin products will not contribute to sales and to "expect further losses." No one is saying what's left but, at this stage, a tangible net asset value count, and that's only 3,7c/share. In terms of the share trading for the 12 months to January, it was at highest 185c and lowest 11c

7. Beige *(Financial Mail 1 October 1999 and 28 January 2000)*

Beige was suspended from trading in the JSE in 1999, at its own request, and a number of its senior executives were suspended.

The group had suffered from excessive and rapid expansion, cash flow pressures, and ineffective executive management and, of course, fraud, theft and accounting misstatements.

There was a possibility of insider trading pointed out by the fact that a 46,000-share/week average trading volume escalated into an average of 2.96 m shares/week from the beginning of September1999. In addition, during the week ended 10 September 1999, the week of the profit warning, astute shareholders managed to offload no less than 6.48m shares, about 7.5% of the total issue, at an average of around 140c/share. A fair premium on Beige's 46c/share price at suspension at end on September. This resulted into investigations by the FSB.

The shareholders were being fed bullish statements and predictions that were not real. Undoubtedly, corporate governance standards and the role of directors were in question

Findings

The closure of investigations into the trading in Beige's shares came after former Beige joint MD Syd Rogers paid R800000 in a move aimed at disposing of the matter. After Rogers's payment to the FSB, further investigations were carried out, then the directorate decided to close the case.

A fraud docket has since been opened against certain directors of Beige. There's no word on the progress, thus far. We consider the Beige case closed, says Barrow, who explains that it is not within the directorates brief to follow up on cases of fraud and irregularities. After the discovery of irregularities within the group, the Beige board recommended the removal of three of its directors from the board and has since steered the company towards a restructuring path, which involved selling some of its business units.

8. **Leisurenet (Health & Racket**) *[Financial mail 13 October 2000]*

Leisurenet (Health & Racket) was put in liquidation in year 2000.

The LeisureNet debacle is that once again the top asset managers and several directors were merrily led down the garden path by executives who did not appear to have the best interest of shareholders at heart.

The company's demise was propelled by irresponsible actions offshore. In the rush to expand the Healthland gym operations offshore, seemingly no cognizance was undertaken of LeisureNet's balance sheet, which did not have the muscle to fund leases and buildings in hard currencies.

9. **Molope Holdings** *[Financial Mail 17 March 2000]*

Due to sidelining the King Report on corporate governance, the share value of Molope group declined to a low of under 90 cents in year 2000 which was far much below the price at which major shareholders bought their shares at R 6/share. In 1998, the shares had hit picks of 910. Its market value dropped from mores than R 1.2billion in late 1998 to about R 210 million in year 2000. In addition, the group was heavily geared and this resulted to entering to a sale deal with Rebhold for sale of 8 subsidiaries at a value of R 300m in year 2000.

The main reasons that eroded the investors' confidence and resulted to the decline in share price (also attributed to poor corporate governance) included: -

(i) Before listing in 1997, Molope went into an acquisition spree and acquired under-performing businesses, particularly in its hospitality division. Proper due diligence investigations were not undertaken on the acquired businesses.

(ii) The published audited financial statements for 30 June 1998 were later found to contain fundamental errors despite the assurance by Molope directors that they "believe that the internal accounting controls are adequate to ensure the reliability and integrity of financial and operating information. Auditors Coopers & Lybrand also certified the Molope's 1998 financial statements "fairly present, in all material respects, the financial position of the company".

Despite this assurance, shareholders were informed a year later, when Molope published the financials for 1999, that 1998 figures had been restated because they contained fundamental errors relating to the warranty that Grantham vendors gave Molope. The warranty stated that Grantham business would report profits of R 14m for financial year 1998 which resulted to 1998 figures being prepared on assumption that the profit warranties were achieved and while actually this was not the case.

(iii) Inadequate and selective disclosure of information to shareholders e.g. Molope directors did not disclose to shareholders that the restraints of trade on some key managers of operating subsidiaries automatically fall away in the case of change of control of Molope.

(iv) Failure by Molope executive directors to give shareholders a detailed breakdown on their interest in the Rebhold deal. A case in point is the restraint of trade agreement 70% of Molope's key managers have now entered into with Rebhold.

10. **Billboard** *(Financial Mail 19 November 1999)*

Billboard share price tanked from a peak of 245c in July 1998 to 8 c in 1999 and earnings fell because of a tough economy and an overweight cost structure.

Billboard listed only in July 1998, but ignored cardinal rules followed to list where the purchase price is settled in shares, with the bulk of payment deferred until generally high profit forecast are met, consisting of eight communication and media businesses.

The merged company promised an aggressive acquisition strategy, lucrative opportunities to earn foreign currency and benefits from "the convergence of communications and information technology industries".

A mere 17 months later, a profit warning issued by the group states its acquisition strategy has caused serious problems. "Costs associated with the group gearing up for new business won are yet unmatched by revenues," it says. The warning adds that there will be lower than expected revenues in the exhibitions, reproduction and print businesses.

The market first realised the severity of Billboard's problems when one business that listed with the group was ousted after failing to meet profit warranties. Closing this business led to a R1,7m provision for losses and more oustings could follow.

But that was just the start of the group's woes. Management is faced with a share price trailing below 10c, failure to meet its earnings forecast earnings growth (25% growth forecast to end-February 2000), the recent departure of CEO Rob Fehrsen and director Michelle Welford-Costelloe in September and the imminent loss of further divisions that are unlikely to meet profit forecasts.

11. **Regal Treasury Private Bank Limited** *(Business Day 28 June 2001)*

Regal Treasury Private Bank Limited ("Regal"), was placed into **curatorship** on 26 June 2001 by the Minister of Finance, in terms of the Banks Act. The reason given by the Registrar of Banks was that recent events had led to unusually large withdrawals by depositors at Regal, which, as a result, was having "difficulties in maintaining its required levels of liquidity."

Regal collapsed after a run on the bank sparked by an announcement of the withdrawal of auditors' support for this year's results, and the cancellation of 45% of its shares.

Jeff Levenstein, the founder and deposed chairman of Regal Private Treasury Bank, has **admitted to lying to his board** as a tactic to prevent the early failure of the bank. *(Business Report 18 September 2001)*

There were **disputes** between the auditors and Regal's management over the **2000 financial accounts**, regarding the accounting of revenue from Regal's **"branding" strategy**. The then Chairman and CEO, Jeff Levenstein, would rather have a qualified audit statement than adjust its revenue. The Registrar of Banks, Christo Wiese pushed the auditors and Bank to resolve their differences. Regal then published the "audited" results over SENS without consulting its auditors, reporting a 50,01c earnings per share figure, but also a 79,96c earnings numbers which Regal said should be on its valuation. The auditors protested and Regal issued a clarification over SENS stating that 50,01c was the correct number - R55m was removed from the income statement. *(Business Day 11 September 2001)*

The **"branding" strategy** involved lending out Regal's brand and banking infrastructure to third parties in exchange for an equity stake. The problem was that Levenstein then valued that equity at alarming amounts, and tried to run it through the income statement.

Levenstein, obsessed with the holding company's share price, instructed the asset management and stock broking businesses in the group not to sell Regal shares under any circumstances a few months after listing.

During the third quarter of 2000, the Reserve Bank commissioned Deloitte & Touche to do a full Section 7 inquiry, the result was produced in October 2000. On corporate governance, Deloittes found a lack of terms of reference for the corporate governance committees, and a lack of independence - Levenstein chaired five of the eight. It found a lack of experience in banking among board members and a lack of qualified and independent executives at the bank. It also found possible contravention of laws.

The corporate **misgovernance** apparently extended to Levenstein's pocket. During 2000 Levenstein forced through an R2m bonus to himself, as a more tax-efficient restraint-of-trade payment. He also won approval for the issue of 500m shares to himself. Those were never actually issued, though he received a R650 000 dividend payment for them. Levenstein also claimed back personal expenses from the bank, including phone bills and speeding fines. He also dished out cars to employees at the bank, telling them they were theirs but including the vehicles on the bank's asset register. *(Financial Mail 19 October 2001)*

12. **Saambou Bank** *(Business Day)*

During January 2002 allegations of insider trading, the publication of the quantum of non-performing loans at a fellow micro-lender combined with adverse ratings granted to A2 banks, culminated in negative sentiment and a **loss of confidence in the bank**. Deposits were withdrawn to such an extent that Saambou was no longer able to fund itself. On 9 February 2002 Saambou was placed under curatorship by the Minister of Finance, in terms of Section 69 of the Bank's Act, 1990."

The share price, which had been falling since the beginning of the week, plummeted by a further 46% in early trade on the JSE Securities Exchange SA yesterday, reaching an intra-day low of R1,20. It later recovered to close at R1,65, down 26% for the day. This compares with a peak of R13,50 in May last year. *(Business Day 7 February 2002)*

Saambou went into curatorship after major investors withdrew more than R1-billion last week and an international ratings agency downgraded the bank and its parent's rating. *(Business Report 11 February 2002)*

C. CORRUPTION

Corruption is one of the oldest white-collar crimes known to mankind. The tradition of paying off of public officials or company employees for preferential treatment roots itself from the crudest business system developed. Bribery could be mankind's second oldest profession. One of the most infamous cases of bribery was that of Judas Iscariot, the disciple who betrayed Jesus Christ. Judas was paid 30 pieces of silver by the chief priests and elders of Jerusalem to disclose the location of Christ during the night so that He could be captured and executed. Judas led an armed guard to the garden of Gethsemane, where he identified Christ by kissing Jesus on the cheek and whispering "Master". The city elders then crucified Christ. Judas was distraught about having betrayed Jesus and gave the silver pieces back and hanged himself shortly after.

In many countries today, corruption must be confronted as a matter of urgency, and often as a prelude to economic growth. Corruption is detrimental both socially and economically whenever and wherever it occurs, without regard to the state of a country's development. The corruption reports unfolding in our newspapers on a daily basis clearly demonstrate that corruption is increasing and is not something that is exclusively, or even primarily, a problem of developing countries. Events in Europe and North America have shown all too clearly that corruption is not a topic on which the industrialized countries can moralize to anyone.

"...all of us know that those intent on committing crime *will continuously seek new ways and means to beat the law enforcement system*," he told government, business and civil society representatives.

The new Prevention and Combating of Corrupt Activities Act contained additional tools to fight corruption, including the encouragement of the public to record corruption and other crimes to the police and the establishment of a register of businesses that committed corrupt acts, especially in government procurement.

"...*to be effective in its efforts to raise awareness, prevent and fight corruption, a mechanism of this nature needs to have a deliberate plan of work, with defined responsibilities and accountability arrangements*," said Mbeki.

"As we know, corruption occurs in all sectors of society. The perpetrators, those corrupting and those corrupted are equally guilty.

While we tend to concentrate on corruption of high value transactions and the dealing of the upper echelons of society, *ordinary people are the most vulnerable* to corruption in the processes of accessing services and infrastructure such as government grants, water, electricity, land and housing." This also applied to those seeking employment or workers unable to gain promotion because of corruption of their supervisors, said Mbeki.

"...we have a particular responsibility to protect the poor and the weak from the corrupt practices of those in powerful positions," he said.

President Mbeki at the 2nd Anti-Corruption Summit, 22 March 2005

So what has gone wrong? Why is corruption rearing its ugly head in more and more ways? The answer lies in a lack of transparency and accountability on the part of public integrity systems. In many countries there is a widespread feeling that the public service has lost its way - that many elements within the public sector are corrupt, and so are many of the private sector firms that transact business with them. The public sees officials, and officials seem to see themselves, as

existing not to provide a service to the public, but as a body that is not accountable to the public they profess to serve. The portrait may be unfair, but the perception is widely held.

Survival tactics in Thailand

One Thai official is reported saying: "What you have called corruption, I call survival. My subordinates count on me to help them in any way possible. I like my job. I am supporting a large family. There may be other ways, but I don't see them and besides, I am not hurting anyone. You tell me what alternatives there are. Do you know my salary? I am not stupid. I know my duty and so does everyone else. Corruption is a problem in Thailand but there's no better way now. Besides, every person in this [section] has been involved [in corruption] for years."

The TI Corruption Perceptions Index

	1995	**1997**	**1999**	**2001**	**2003**
Highest score	9.55	9.94	10.00	9.90	9.70
Highest scoring country	New Zealand	Denmark	Denmark	Finland	Finland
Lowest score	1.94	1.76	1.50	1.00	1.30
Lowest scoring country	Indonesia	Nigeria	Cameroon	Bangladesh	Bangladesh
South Africa	5.62	4.95	5.00	4.80	4.40
South Africas position	21	33	34	39	49
Nigeria *	-	1.76	1.60	1.00	1.40
U.S.A *	7.79	7.61	7.50	7.60	7.50
No. of countries surveyed	41	52	99	91	133

Source: Transparency International's Internet website
* Included for comparative purposes

Notes:

CPI Score - relates to perceptions of the degree of corruption as seen by business people, risk analysts and the general public and ranges between 10 (highly clean) and 0 (highly corrupt).

Surveys Used - refers to the number of surveys that assessed a country's performance. 16 surveys were used and at least 3 surveys were required for a country to be included in the CPI.

Transparency International - http://www.transparency.org

OECD (Organization for Economic Co-operation & Development) – http://www.oecd.org

The Myth Of Culture

One way to justify bribery is with the "culturally relativistic" argument. It is often suggested in developed countries that corruption is part of the "culture" of many developing countries. The fact that people in a particular country may tolerate demands for small payments in return for official services (e.g., the issuing of permits, licenses, etc.) does not necessarily imply that they approve of it; it may simply be that the public "perceive it as the most workable way of obtaining things they want or need...[a] perception that may gradually be undermined by rising prices... or dashed more abruptly if consumers come to believe that the underlying scarcities are artificially contrived or that more desirable alternative processes are really possible."

Yet, one could ask why there are laws against corruption in all countries, developed or developing, if, in fact, it is "a part of their culture"? Why, too, one might inquire, have the people of the Philippines and Bangladesh mobilized against a well-armed military to bring down corrupt leaders? These events hardly square with a popular acceptance of corruption as "a part of culture."

Budget Fraud In The European Union

Most Europeans would reject any suggestion that corruption was "a part" of European culture, yet there is an impressive array of evidence that could be employed to support this charge. One need not point only to the political and "big business" corruption scandals that have effectively destabilized Italy and Spain, and which more recently have surfaced in France. Fraud against the budget of the European Union has become a major problem, and increasingly instances are surfacing of bribes being paid to public officials in public procurement among European countries.

In some cases, corruption may reflect practices introduced to a culture by a foreign power. Indonesia is beset by massive corruption. Yet some writers have noted that this phenomenon originated, not with the Indonesians, but with the Dutch East India Company. The company's men "were underpaid and exposed to every temptation that was offered by the combination of a weak native organization, extraordinary opportunities in trade, and an almost complete absence of checks from home or in Java. Officials became rich by stealing from the company. "

The same writer notes "corruption was introduced into [the Philippines] during the Spanish colonial period. He also notes that in Singapore after World War Two, "the British Army officers in charge of local purchases had probably never before been exposed to the type of temptations in money, wine and women...whatever resistance there was in them melted away with mercurial speed."

The author also notes that Thailand is the only ASEAN country that has not been colonized. "However, freedom from colonial domination does not guarantee that a country will be immune to the disease of corruption. Indeed, in Thailand's case corruption is an endemic disease which can be traced to the corrupt behavior of the government officials belonging to the sixteenth century bureaucracy."

Similar origins have been attributed to corruption on the African continent. One writer observes: "when we look at what we see it is only fair to reflect on the state of affairs which African countries inherited on gaining independence. Colonialism was marked by a lack of accountability--other than to London, Paris, Lisbon, Berlin or Rome. It was marked by an absence of transparency. The courts

existed, not to do justice and enforce the rule of law, but to sustain the imposition of colonialism. The judges were simply civil servants wearing wigs. And the style of governance was characterized by government being "done" to the people, rather than a people being governed by consent--and the instruments of repression were handed over, intact, to the incoming administrations. Against such a background, the positive achievements of some African countries have been little short of astonishing".

Today, of course, there are significant differences in perceptions and practices between various cultures. What some accept as reasonable and appropriate will differ very widely. These differences, however, may have more to do with how business is conducted (through the giving of presents and of hospitality) than with blatant attempts to "buy" favourable decisions. There is a clear distinction between "reciprocity" and reciprocities classified as bribes. In the African context, the suggestion that there is a cultural explanation for lavish gift-giving in return for favours bestowed has been robustly attacked by General Obasanjo, former head of government of Nigeria:

"I shudder at how an integral aspect of our culture could be taken as the basis for rationalizing otherwise despicable behaviour. In the African concept of appreciation and hospitality, the gift is usually a token. It is not demanded. The value is usually in the spirit rather than in the material worth. It is usually done in the open, and never in secret. Where it is excessive, it becomes an embarrassment and it is returned. If anything, corruption has perverted and destroyed this aspect of our culture."

In the Far East, too, the complaint is that traditional practices have been subverted. "Once, the exchanging of gifts was a laudable social custom emphasizing the importance of personal relations in social life. Now, Korean leaders have distorted the practice into institutionalized bribery in the name of goodwill tokens."

One conclusion that provides a succinct riposte to apologists for corruption being simply cultural is this: the public men on whom wealth has descended in a sudden and unimaginable torrent are not heirs to a tradition of comfortable bank balances and public responsibility; they are nouveaux rich tycoons of public administration - those who happened to be in the right place at the right time.

The Consequences of Accepting Bribes

Gordon Foxley, a civil servant at Britain's Ministry of Defense, was imprisoned for four years for taking at least US$2.25 million in bribes. But in an analysis carried out for TI-UK, he is said to have caused up to US$200 million in financial damage. This included the cost of job losses at the factory in Britain which failed to gain the orders (they went abroad), loss of profit s leading to lower values for privatization exercises, the loss of highly-developed skills, the higher price paid than was necessary, and the purchase in at least one instance of a fuse which was useless as it was "ineffective in practice and battle conditions".

Corruption defined

Defined simply, corruption is the misuse of public power for private profit. However, definitions of corruption and its impact will vary. One cannot assume that corruption always means the same thing or has the same impact or motivation. Normative statements about corruption require a point of view, a standard of "goodness" and a model of how corruption works in particular instances.

For the purposes of this workbook, "corruption" involves behaviour on the part of officials in the public sector, whether politicians or civil servants, in whom they improperly and unlawfully enrich themselves, or those close to them, by the misuse of the public power entrusted to them. The workbook concentrates on administrative rather than political corruption per se, focusing on the activities of individuals who, in their positions as public officials - as policy-makers or as administrators - control various activities or decisions.

There are two quite separate categories of administrative corruption: the first occurs where, for example, services or contracts are provided "according-to-rule" and the second, where transactions are "against-the-rule." In the first situation, an official is receiving private gain illegally for doing something that he or she is ordinarily required to do by law. In the second situation, the bribe is paid to obtain services that the official is prohibited from providing. "According-to-rule" and "against-the-rule" corruption can occur at all levels of the government hierarchy and range in scale and impact from "grand corruption" to more ordinary, small-scale varieties. In practice, public attitudes can overshadow legal definitions of administrative corruption, and public opinion can define corruption in ways which will over-ride law. If public opinion and legal definitions do not conform, the likelihood is that officials will act in accordance with the public view, and in so doing transgress the law. It is therefore crucial that the public be informed and enlightened as to the damage that corruption can cause.

Corruption can take many forms, including:

1. **Conflict of interest:** where an official stands to profit incidentally from an official act. This could involve an official awarding a contract to a company in which the official has a financial interest.

2. **Bribery:** where an official accepts money or some other consideration to engage in a particular course of action, or inaction.

3. **Illegal Gratuities:** are similar to bribery schemes except there is not necessarily an intent to influence a particular business decision.

4. **Economic Extortion:** where an official demands money or some other consideration to engage in a particular course of action, or inaction.

Keep in mind that corruption is not be limited to the public sector. Officers of large companies may use its resources for private purposes, and other employees may be party to the activities just described above.

CONFLICTS OF INTEREST

Types of Schemes

The majority of the conflicts schemes in the ACFE survey fit into two categories: purchases schemes and sales schemes. In other words, most conflicts of interest arise when a victim company unwittingly buys something at a high price from a company in which one of its employees has a hidden interest, or unwittingly sells something at a low price to a company in which one of its employees has a hidden interest. Most of the other conflicts involved employees who stole clients or diverted funds from their employer.

PURCHASES SCHEMES

The majority of conflicts schemes in the ACFE study were purchase schemes and the most common of these was the over billing scheme. While it is true that any time an employee assists in the over billing of his company there is probably some conflict of interest (the employee causes harm to his employer because of a hidden financial interest in the transaction), this does not necessarily mean that every false billing will be categorized as a conflict scheme. In order for the scheme to be classified as a conflict of interest, the employee (or a friend or relative of the employee) must have some kind of ownership or employment interest in the vendor that submits the invoice. This distinction is easy to understand if we look at the nature of the fraud. Why does the fraudster over bill his employer? If he engages in the scheme only for the cash, the scheme is a fraudulent disbursement-billing scheme. If, on the other hand, he seeks to better the financial condition of his business at the expense of his employer, this is a conflict of interest. In other words, the fraudster's interests lie with a company other than his employer. When an employee falsifies the invoices of a third-party vendor to whom he has no relation, this is not a conflict of interest scheme because the employee has no interest in that vendor. The sole purpose of the scheme is to generate a fraudulent disbursement.

Unique Assets

Not all conflicts schemes occur in the traditional vendor-buyer relationship. Several of the cases in our survey involved employees negotiating for the purchase of some unique, typically large asset such as land or a building in which the employee had an undisclosed interest. It is in the process of these negotiations that the fraudster violates his duty of loyalty to his employer. Because he stands to profit from the sale of the asset, the employee does not negotiate in good faith to his employer; he does not attempt to get the best price possible. The fraudster will reap a greater financial benefit if the purchase price is high.

Turnaround Sales

A special kind of purchasing scheme that was encountered in the ACFE study is called the turnaround sale or flip. In this type of scheme an employee knows his employer is seeking to purchase a certain asset and takes advantage of the situation by purchasing the asset himself (usually in the name of an accomplice or shell company). The fraudster then turns around and resells the item to his employer at an inflated price.

SALES SCHEMES

The ACFE study has identified two principal types of conflicts schemes associated with the victim company's sales. The first and most harmful is the underselling of goods or services. Just as a corrupt employee can cause his employer to overpay for goods or ser vices sold by a company in which he

has a hidden interest, so too can he cause the employer to undersell to a company in which he maintains a hidden interest.

Under billings
The perpetrator under-bills the vendor in which he has a hidden interest. The victim company ends up selling its goods or ser vices below fair market value, which results in a diminished profit margin or even a loss on the sale, depending upon the size of the discount.

Writing off Sales
The other type of sales scheme involves tampering with the books of the victim company to decrease or write off the amount owed by an employee's business. For instance, after an employee's company purchases goods or services from the victim company, credit memos may be issued against the sale, causing it to be written off to contra accounts such as Discounts and Allowances. The fraudster could assist favoured clients by delaying billing on their purchases for up to 60 days. When the receivable on these clients' accounts become delinquent, the perpetrator can issue credit memos against the sales to delete them. A large number of reversing entries to sales may be a sign that fraud is occurring in an organization. The fraudster could avoid the problem of too many write-offs by issuing new invoices on the sales after the "old" receivables were taken off the books. In this way the receivables could be carried indefinitely on the books without ever becoming past due.

OTHER SCHEMES

In other cases the perpetrator might not write off the scheme, but simply delay billing. This is sometimes done as a "favour" to a friendly client and is not an outright avoidance of the bill but rather a delaying tactic. The victim company eventually gets paid, but loses time value on the payment that arrives later than it should.

Business Diversions
An employee could start his own business that would compete directly with his employer. While still employed by the victim company, this employee could begin siphoning off clients for his own business. This activity would clearly violate the employee's duty of loyalty to his employer. There is nothing unscrupulous about free competition, but while a person acts as a representative of his employer it is certainly improper to try to undercut the employer and take his clients. There is nothing unethical about pursuing an independent venture (in the absence of restrictive employment covenants such as non compete agreements) but if the employee fails to act in the best interests of his employer while carrying out his duties, then this employee is violating the standards of business ethics.

"Let the buyer beware", *(Caveat Emptor), has been changed to:*

"Beware of the Buyer!"

Resource Diversions
Finally, some employees divert the funds and other resources of their employers to the development of their own business.

Financial Disclosures
Management has an obligation to disclose to the shareholders significant fraud committed by officers, executives, and others in positions of trust. Management does not have the responsibility of disclosing uncharged criminal conduct of its officers and executives. However, if and when officers, executives, or other persons in trusted positions become subjects of a criminal indictment, disclosure is required. The inadequate disclosure of conflicts of interests is among the most serious of frauds. Inadequate disclosure of related-party transactions is not limited to any specific industry; it transcends all business types and relationships.

Conclusion

Following the old saying of an ounce of prevention being worth a pound of cure, conflict of interest cases are more easily prevented than detected. There are internal controls which make it much more difficult for employees to run this kind of scheme.

BRIBERY

KICKBACK SCHEMES

Kickback schemes involve the submission of invoices for goods and services that are either overpriced or completely fictitious. Kickbacks are classified as corruption schemes rather than asset misappropriations because they involve collusion between employees and vendors. In a common type of kickback scheme, a vendor submits a fraudulent or inflated invoice to the victim company and an employee of that company helps make sure that a payment is made on the false invoice. For his assistance, the employee-fraudster receives some form of payment from the vendor. This payment is the kickback. Kickback schemes almost always attack the purchasing function of the victim company, so it stands to reason that employees with purchasing responsibilities often undertake these frauds. Purchasing employees often have direct contact with vendors and therefore have an opportunity to establish a collusive relationship.

Diverting Business to Vendors
In some instances, an employee-fraudster receives a kickback simply for directing excess business to a vendor. There might be no over billing involved in these cases; the vendor simply pays the kick backs to ensure a steady stream of business from the purchasing company. If no over billing is involved in a kickback scheme, one might wonder where the harm lies. Assuming the vendor simply wants to get the buyer's business and does not increase his prices or bill for undelivered goods and services, how is the buyer harmed? The problem is that, having bought off an employee of the purchasing company, a vendor is no longer subject to the normal economic pressures of the marketplace. This vendor does not have to compete with other suppliers for the purchasing company's business, and so has no incentive to provide a low price or quality merchandise. In these circumstances the purchasing company almost always ends up over paying for goods or services, or getting less than it paid for. Once a vendor knows it has an exclusive purchasing arrangement, his incentive is to raise prices to cover the cost of the kickback. Most bribery schemes end up as over billing schemes even if they do not start that way. This is one reason why most business codes of

ethics prohibit employees from accepting undisclosed gifts from vendors. In the long run, the employee's company is sure to pay for his unethical conduct.

Over billing Schemes

Employees with Approval Authority
In most instances, kickback schemes begin as over billing schemes in which a vendor submits inflated invoices to the victim company. The false invoices either overstate the cost of actual goods and services, or reflect fictitious sales. The ability to authorize purchases (and thus to authorize fraudulent purchases) is usually a key to kickback schemes. The existence of purchasing authority can be critical to the success of kickback schemes. The ability of a fraudster to authorize payments himself means he does not have to submit purchase requisitions to an honest superior who might question the validity of the transaction.

Fraudsters Lacking Approval Authority
While the majority of the kickback schemes that the ACFE reviewed involved people with authority to approve purchases, this authority is not an absolute necessity. When an employee cannot approve fraudulent purchases himself, he can still orchestrate a kickback scheme if he can circumvent accounts payable controls. In some cases, all that is required is the filing of a false purchase requisition. If a trusted employee tells his superior that the company needs certain materials or services, this is sometimes sufficient to get a false invoice approved for payment. Such schemes are generally successful when the person with approval authority is inattentive or when he is forced to rely on his subordinates' guidance in purchasing matters.
Corrupt employees might also prepare false vouchers to make it appear that fraudulent invoices are legitimate. Where proper controls are in place, a completed voucher is required before accounts payable will pay an invoice. One key is for the fraudster to create a purchase order that corresponds to the vendor's fraudulent invoice. The fraudster might forge the signature of an authorized party on the purchase order to show that the acquisition has been approved. Where the payables system is computerized, an employee with access to a restricted password can enter the system and authorize payments on fraudulent invoices. In less sophisticated schemes, a corrupt employee might simply take a fraudulent invoice from a vendor and slip it into a stack of prepared invoices before they are input into the accounts payable system.
Kickback schemes can be very difficult to detect. In a sense, the victim company is being attacked from two directions. Externally, a corrupt vendor submits false invoices that induce the victim company to unknowingly pay for goods or services that it does not receive. Internally, one or more of the victim company's employees waits to corroborate the false information provided by the vendor.

Other Kickback Schemes

Bribes are not always paid to employees to process phony invoices. In some circumstances outsiders seek other fraudulent assistance from employees of the victim company. In these other cases, bribes come not from vendors who are trying to sell something to the victim company, but rather from potential purchasers who seek a lower price from the victim company.

Slush Funds
It should also be noted that every bribe is a two-sided transaction. In every case where a vendor bribes a purchaser, there is someone on the vendor's side of the transaction who is making an illicit payment. It is therefore just as likely that your employees are paying bribes as accepting them. In

order to obtain the funds to make these payments, employees usually divert company money into a slush fund, a non-company account from which bribes can be made. Assuming that the briber's company does not authorize bribes, he must find a way to generate the funds necessary to illegally influence someone in another organization. Therefore, the key to the crime from the briber's perspective is the diversion of money into the slush fund. This is a fraudulent disbursement of company funds, which is usually accomplished by the writing of company checks to a fictitious entity or the submitting of false invoices in the name of the false entity. It is common to charge fraudulent disbursements to 'hazy' accounts like "consulting fees." The purchase of goods can be verified by a check of inventory, but there is no inventory for these kinds of services. It is therefore more difficult to prove that the payments are fraudulent.

BID-RIGGING SCHEMES

As we have said, when one person pays a bribe to another, he does so to gain the benefit of the recipient's influence. The competitive bidding process, in which several suppliers or contractors are vying for contracts in what can be a very cutthroat environment, can be tailor-made for bribery. Any advantage one vendor can gain over his competitors in this arena is extremely valuable. The benefit of "inside influence" can ensure that a vendor will win a sought-after contract. Many vendors are willing to pay for this influence.

In the competitive bidding process, all bidders are legally supposed to be placed on the same plane of equality, bidding on the same terms and conditions. Each bidder competes for a contract based on the specifications set forth by the purchasing company. Vendors submit confidential bids stating the price at which they will complete a project in accordance with the purchaser's specifications.

The way competitive bidding is rigged depends largely upon the level of influence of the corrupt employee. The more power a person has over the bidding process, the more likely the person can influence the selection of a supplier. Therefore, employees involved in bid-rigging schemes, like those in kickback schemes, tend to have a good measure of influence or access to the competitive bidding process. Potential targets for accepting bribes include buyers, contracting officials, engineers and technical representatives, quality or product assurance representatives, subcontractor liaison employees, or anyone else with authority over the awarding of contracts.

Bid-rigging schemes can be categorized based on the stage of bidding at which the fraudster exerts his influence. Bid-rigging schemes usually occur in the pre-solicitation phase, the solicitation phase, or the submission phase of the bidding process.

The Pre-Solicitation Phase

In the pre-solicitation phase of the competitive bidding process - before bids are officially sought for a project - bribery schemes can be broken down into two distinct types. The first is the need recognition scheme, where an employee of a purchasing company is paid to convince his company that a particular project is necessary. The second reason to bribe someone in the pre-solicitation phase is to have the specifications of the contract tailored to the strengths of a particular supplier.

Need Recognition Schemes

The typical fraud in the need recognition phase of the contract negotiation is a conspiracy between the buyer and contractor where an employee of the buyer receives something of value and in return recognizes a "need" for a particular product or service. The result of such a scheme is that the victim company purchases unnecessary goods or services from a supplier at the direction of the corrupt employee.

There are several trends that may indicate a need recognition fraud. Unusually high requirements for stock and inventory levels may reveal a situation in which a corrupt employee is seeking to justify unnecessary purchase activity from a certain supplier. An employee might also justify unnecessary purchases of inventory by writing off large numbers of surplus items to scrap. As these items leave the inventory, they open up spaces to justify additional purchases. Another indicator of a need recognition scheme is the defining of a "need" that can only be met by a certain supplier or contractor. In addition, the failure to develop a satisfactory list of backup suppliers may reveal an unusually strong attachment to a primary supplier - an attachment that is explainable by the acceptance of bribes from that supplier.

Specifications Schemes

The other type of pre-solicitation fraud is a specifications scheme. The specifications of a contract are a list of the elements, materials, dimensions, and other relevant requirements for completion of the project. Specifications are prepared to assist vendors in the bidding process, telling them what they are required to do and providing a firm basis for making and accepting bids.

One corruption scheme that occurs in this process is the fraudulent tailoring of specifications to a particular vendor. In these cases, the vendor pays off an employee of the buyer who is involved in the preparation of specifications for the contract. In return, the employee sets the specifications of the contract to accommodate that vendor's capabilities.

The methods used to restrict competition in the bidding process may include the use of "pre-qualification" procedures that are known to eliminate certain competitors. For instance, the bid may require potential contractors to have a certain percentage of female or minority ownership. There is nothing illegal with such a requirement, but if it is placed in the specifications as a result of a bribe rather than as the result of other factors, then the employee has sold his influence to benefit a dishonest vendor, a clear case of corruption. Sole-source or noncompetitive procurement justifications may also be used to eliminate competition and steer contracts to a particular vendor.

Another type of specifications scheme is the deliberate writing of vague specifications. In this type of scheme, a supplier pays an employee of the purchasing company to write specifications that will require amendments at a later date. This will allow the supplier to raise the price of the contract when the amendments are made. As the buyer's needs become more specific or more detailed, the vendor can claim that, had he known what the buyer actually wanted, his bid on the project would have been higher. In order to complete the project as defined by the amended specifications, the supplier will have to charge a higher price.

Another form of specifications fraud is bid splitting where an employee splits a large job into several component contracts in order to divert the jobs to his brother in-law. Each sectional project’s cost comes in below the mandatory bidding level and so the brother-in-law gets the entire contract while avoiding competitive bidding.

A less shocking but nevertheless unfair form of bid rigging occurs when a vendor pays an employee of the buyer for the right to see the specifications earlier than his competitors. The employee does not alter the specifications to suit the vendor, but instead simply gives him a head start on planning his bid and preparing for the job. The extra planning time gives the vendor an advantage over his competitors in preparing a bid for the job.

The Solicitation Phase

In the solicitation phase of the competitive bidding process fraudsters attempt to influence the selection of a contractor by restricting the pool of competitors from whom bids are sought. In other words, a corrupt vendor pays an employee of the purchasing company to assure that one or more of

the vendor's competitors do not get to bid on the contract. Therefore, the corrupt vendor is able to improve his chances of winning the job.

One type of scheme involves the sales representative who deals on behalf of a number of potential bidders. The sales representative bribes a contracting official to rig the solicitation, ensuring that only those companies represented by him get to submit bids. It is not uncommon in some sectors for buyers to "require" bidders to be represented by certain sales or manufacturing representatives. These representatives pay a kickback to the buyer to protect their clients' interests. The result of this transaction is that the purchasing company is deprived of the ability to get the best price on its contract. Typically, the group of "protected" vendors will not actually compete against each other for the purchaser's contracts, but instead engage in "bid pooling."

Bid Pooling

Bid pooling is a process by which several bidders conspire to split contracts up and ensure that each gets a certain amount of work. Instead of submitting confidential bids, the vendors discuss what their bids will be so they can guarantee that each vendor will win a share of the purchasing company's business. For example, if vendors A, B, and C are up for three separate jobs, they may agree that A's bid will be the lowest on the first contract, B's bid will be the lowest on the second contract, and C's bid will be the lowest on the third con tract. None of the vendors gets all three jobs, but on the other hand, they are all guaranteed to get at least one. Furthermore, since they plan their bids ahead of time, the vendors can conspire to raise their prices. Thus the purchasing company suffers as a result of the scheme.

Fictitious Suppliers

Another way to eliminate competition in the solicitation phase of the selection process is to solicit bids from fictitious suppliers. A supplier could submit quotes in the names of several different companies and could even perform work under these various names. The employee will use the quotes from several of his friend’s fictitious companies to demonstrate price reasonableness on the final contracts. In other words, the fictitious price quotes were used to validate the actual prices.

Other Methods

In some cases, competition for a contract can be limited by severely restricting the time for submitting bids. Certain suppliers are given advance notice of contracts before bids are solicited. These suppliers are therefore able to begin preparing their bids ahead of time. With the short time frame for developing bid proposals, the supplier with advance knowledge of the contract will have a decided advantage over his competition.

Bribed purchasing officials can also restrict competition for their co-conspirators by soliciting bids in obscure publications where other vendors are unlikely to see them. Again, this is done to eliminate potential rivals and create an advantage for the corrupt suppliers. Some schemes have also involved the publication of bid solicitations during holiday periods when those suppliers not "in the know" are unlikely to be looking for potential contracts. In more blatant cases, the bids of outsiders are accepted but are "lost" or improperly disqualified by the corrupt employee of the purchaser.

Typically, when a vendor bribes an employee of the purchasing company to assist him in any kind of solicitation scheme, the cost of the bribe is included in the corrupt vendor's bid. Therefore, the purchasing company ends up bearing the cost of the illicit payment in the form of a higher contract price.

The Submission Phase

In the actual submission phase of the process, where bids are proffered to the buyer, several schemes may be used to win a contract for a particular supplier. The principle offense tends to be abuse of the sealed-bid process. Competitive bids are confidential; they are, of course, supposed to remain sealed until a specified date at which all bids are opened and reviewed by the purchasing company. The person or persons who have access to sealed bids are often the targets of unethical vendors seeking an advantage in the process.

Vendors also bribe employees of the purchaser for information on how to prepare their bid. Other reasons to bribe employees of the purchaser include ensuring receipt of a late bid or falsifying the bid log, to extend the bid opening date, and to control bid openings.

ILLEGAL GRATUITIES

Illegal gratuities are similar to bribery schemes except there is not necessarily intent to influence a particular business decision. For example, the corrupt employee gets rewarded with a free international vacation, all-expenses paid. While the promise of this trip may have influenced the negotiations, this would be difficult to prove. However, merely accepting such a gift amounts to an illegal gratuity, an act that is prohibited by most government and private company codes of ethics.

ECONOMIC EXTORTION

Economic extortion is basically the flipside of a bribery scheme. Instead of a vendor offering payment to an employee to influence a decision, the employee demands a payment from a vendor in order to make a decision in that vendor’s favor. In any situation where an employee might accept bribes to favor a particular company or person, the situation could be reversed to a point where the employee extorts money from a potential purchaser or supplier. Those honest suppliers that do not ‘Play Ball’ will lose their business with the company.

Conclusion

Keep in mind that the most telling aspect of corruption is the recipient's lifestyle; they simply don't have the income to support their "fast lane" life. The most important person in a corruption matter is the whistle blower, who has direct knowledge of the illicit payments, and the most important person in the pursuit of bribery and corruption is the investigator. Successful resolution will usually hinge on the detective's ability to follow the money and conduct a successful resolution interview.

There are ways of gathering evidence of income from illicit transactions. The Net Worth method is used to show that the subject’s assets or expenditures for a given period exceed that which can be accounted for from admitted sources of income. The Net Worth ASSET method is used when the subject has invested illegal funds to accumulate wealth and acquire assets, causing net worth (value of assets over liabilities) to increase from year to year. The Net Worth EXPENDITURES method is best used when the subject spends illicit income on consumables that would not cause an increase in net worth. Both methods are begun by assembling the personal profile. The personal profile consists of 1) the financial profile (a financial statement that shows what the subject earns, owns, owes and spends) and 2) the behavioural profile (the personal habits of the subject).

This method was first successfully used in the tax fraud case of Al Capone. The investigator adds up all assets and subtracts all liabilities of the subject to calculate net worth. Changes in net worth from one period to another must equal the subject's net income. A danger in using this method is that (a) the initial or base net worth figure may be understated due to hidden assets, or (b) subsequently obtained assets may not be visible to the investigator.

Expedited Service in Ecuador

In Ecuador, the average person can take several days to obtain even a simple driver's licence. This is because of lengthy queues, and often a suspicion that civil servants benefit from the commissions paid to 'îagentsï' who are able to go to the head of a queue and expedite service for those who will pay. Those who cannot afford to pay, wait. With the assistance of a 'tramitador', who may even bypass a queue completely and on occasions go behind a civil servant's desk and process an application himself; it can take the applicant only a matter of minutes.

But it is true that in many countries, leaders are of two minds. They may appreciate and decry the costs of systematic corruption. But they may also recognize the personal and party benefits of the corrupt system. To assist them in moving toward a long-term strategy, several almost psychological steps are necessary.

- First, leaders must see that ***improvements are possible without political suicide***. Here is where sensitive consulting and assistance may help leaders learn from anti-corruption efforts elsewhere, take a systematic approach, and analyze confidentially the many categories of political benefits and costs.

- Second, leaders must develop ***a strategy that recognizes that not everything can be done at once***. One should undertake, behind closed doors, a kind of benefit-cost analysis, assessing those forms of corruption where the economic costs are the greatest (for example, corruption that distorts policies as opposed to who gets a specific contract) but also taking into account where it is easiest to make a difference. The anti-corruption effort might begin where the public perceives the problem acutely. A good rule of thumb is that to be credible an anti-corruption campaign must have some tangible successes within six months.

- Third, ***leaders need political insulation***. International collaboration can help provide it, as countries together admit a common problem and move to address it ("corruption is not just our problem, or my party's,"). Indeed, international conditionality that applies across many countries might help a national leader justify anti-corruption measures that might otherwise be embarrassing, or difficult to make credible.

Keep in mind that Corruption is a System and secondly is a crime of calculation, not passion. True, there are saints who resist all temptations, and honest officials who resist most. But when the size of the bribe is large, the chances of being caught small, and the penalty if caught meager, many officials will succumb.

Combating corruption, therefore, begins with better systems. Monopolies must be reduced or carefully regulated. Official discretion must be clarified. Transparency must be enhanced. The probability of being caught must increase, and the penalties for corruption (for both givers and takers) must rise.

Each of these headings introduces a vast topic. But notice that none immediately refers to what most of us think of first when corruption is mentioned - new laws, more controls, a change in mentality, and an 'ethical revolution'. Laws and controls prove insufficient when systems are not there to implement them. Moral awakenings do occur, but seldom by the design of our public leaders. If we cannot engineer incorruptible officials and citizens, we can nonetheless foster competition, change incentives, enhance accountability:- in short, fix the systems that breed corruption.

"I do not think I am overstating anything when I say that this phenomenon (of corruption) can truly be likened to a **cancer eating away remorselessly at the fabric of corporate privity and extending its baleful effect into all aspects of administrative functions, whether state official or private sector manager**," the judge said.

"If it is not checked, it becomes systemic.

And the after-effects of systemic corruption can quite readily extend to the corrosion of any confidence in the integrity of anyone who has a duty to discharge, especially a duty to discharge to the public."

High Court Judge Hilary Squires in sentencing businessman Schabir Shaik
8 June 2005

D. ASSET MISAPPROPRIATION

INVENTORY AND ALL OTHER ASSETS

Most asset misappropriation schemes involve cash, but other assets like inventory supplies, and fixed assets, can be stolen as well. These schemes can range from theft of a box of pens to millions of rands worth of merchandise. Employees can misappropriate a non-cash asset through two basic methods. One is to 'borrow' (misuse) it and the other is to steal it.

Misuse of fixed assets – Misuse commonly occurs with fixed assets such as company cars, computers, the internet, and other office equipment. These assets are used by employees to do personal work in company time. In many cases these side businesses are the same as the employer's business, so the employee is actually competing with his employer and using the employer's equipment to do it.

Theft of inventory, supplies and fixed assets – The most common methods of stealing non-cash assets are:

- ***Fraudulent requisitions and transfers*** – employees can falsify internal documents that deal with the requisition or internal movement of non-cash assets so that they can steal them. They use these documents to justify the transfer or re-allocation of inventory, supplies or assets by enabling them access to items they otherwise might not be able to reach.

- ***Fraudulent shipments of merchandise*** – employees can misappropriate inventory by creating false sales orders or other shipping documents. These false documents represent 'sales' to fictitious persons/companies, or accomplices of the fraudster. The victim organisation's shipping department sends out the inventory that is delivered to the fraudster. If the 'sale' is made to a fraudulent company, the fraudster might not intercept the shipping notice, but let it go forward (and create corresponding support documentation) and allow a receivable to be created. The receivable will eventually be written off to discounts, bad debt or similar account as in some cases the employee has the authority to make these adjustments.

- ***Falsified receiving reports*** – employees can falsify receiving reports or skim goods from incoming deliveries.

- ***Unconcealed larceny*** – employees take company assets from the victim organisation's premises without attempting to conceal the theft in the victim's books. Assets are taken in plain sight during normal business hours, after hours, or with the 'approval' of colleagues who have a 'management vs. labour' mentality. In many cases the items are mailed to an off-site location where the items can be collected far away from corporate security.

CASH THEFT SCHEMES

Theft is defined as 'the unlawful act of taking property without the owner's consent'. A fraudster can misappropriate cash from his employer in two ways:

One is to trick the employer into making a payment for a fraudulent purpose, for example, an employee may produce a fraudulent invoice and based on the false information, the company issues a payment. This is known as a **fraudulent disbursement of cash.**

A second way to misappropriate cash is to physically remove it from the company through a method other than the normal disbursement process. As an example the fraudster may take cash out of his cash register or remove some cash from the bank deposit. This type of misappropriation is referred to as a **cash theft scheme**.

Cash theft schemes can be divided into two categories –

Larceny – is the theft of cash ***after*** it has been recorded in the company accounting system. Obviously it makes more sense to steal cash before it hits an organisation's books because the theft doesn't leave a direct audit trail. That does not mean that employees do not steal incoming funds after they have been recorded. **Cash on hand** can be taken with no attempt to conceal the theft, records of the sales transaction can be destroyed or altered, new sales records can be fabricated, cash can be taken from another employee's register, or sales can be understated. Another area where cash larceny most frequently occurs in the **deposit process**. At some point in every revenue-generating business, someone must physically transport the organisation's currency and cheques to the bank. This person left alone and literally 'holding the bag', will have an opportunity to take a portion of the money prior to depositing it into the organisation's accounts.

Skimming – is the removal of cash from a company ***before*** the cash is entered into an accounting system. Employees who skim from their organisations steal sales or receivables before they are recorded in the company books. Skimming typically involves the theft of sales or receivables, and can occur at any point where funds enter a business. Therefore anyone who deals with the process of receiving cash may be in a position to skim money – this includes salespeople, tellers, cashiers, waiters, and employees who receive and log mail payments.

Most employees will skim sales as the victim organization doesn't 'know' that it ever had the money. Skimming receivables, however, is more difficult as a receivable represents an amount of money owed to an organization. The payment is expected by the organization. If a payment on a receivable is stolen it becomes past due and collection efforts will be made. The fraudster then has to use a number of techniques to conceal the thefts. These techniques could be the forcing of account balances, destroying transaction records, writing off account balances, debiting fictitious accounts, or lapping.

Lapping is one of the most common methods of concealing receivables skimming. Suppose a company has 3 clients, A, B, & C. When A's payment is received the fraudster takes it for himself. When B's cheque arrives the fraudster posts it to A's account. When C's payment is received the fraudster applies it to B's account and the process continues indefinitely.

REGISTER DISBURSEMENTS

False voids and false refunds represent a hybrid class of occupational fraud that lies between cash theft and fraudulent disbursements. Because these schemes appear on the books as legitimate disbursements of funds from the cash register, they are classified as fraudulent disbursements.

A fraudulent refund or void allows the fraudster to take cash from the till without creating an imbalance on the books. Refunds of nonexistent sales are the most common forms of fraudulent register disbursements. The cashier would fill in a refund slip using a random name and address. Another scheme involves employees removing merchandise from the stockroom before it has been sold, and the employee gives it to an accomplice who takes it back to the store for a refund. The money is then split between the two. While false refunds may involve the creation of fictitious sales transactions, voided sales schemes usually target actual sales. An employee will void a sale after a customer has left the store and the employee keeps the money. In other cases employees will overstate the amount of a legitimate refund.

Some of the typical ways in which register disbursements can occur are as follows:

- ***Failure to require approval*** on register refunds and voids.

- ***Rubber-stamp managers*** – Many fraudulent voids occur because negligent managers simply fail to verify the authenticity of the transactions they should be approving. It is not a coincidence that the fraudsters tend to present their void slips to a manager who is known to be complacent about controls.

- ***Forged approval*** – Some employees will simply forge the manager's signature.

- ***Collusion with a manager*** – When a manager is part of the scheme, one control component is missing and the scheme will be more difficult to detect.

- ***Refunds and voids below the minimum approval limit*** – While anti-fraud controls are important, they must be balanced with the business' interest in seeing that customers can receive refunds without too much inconvenience. For efficiency's sake, many companies set limits below which management review of a refund or void is not required. Here fraudsters simply enter multiple refunds that are small enough to be processed without review.

- ***Credit card refunds*** – Some fraudsters process false refunds on credit card sales instead of processing a cash transaction. The benefit of this is that the perpetrator doesn't have to physically take cash from the register and carry it out of the store where colleagues, managers or CCTV cameras may detect the fraudster. The fraudster will ring up a refund on a credit card sale, even though thee is no merchandise being returned, and he will use his or a friend's credit card number.

- ***Destroying transaction records*** – When an employee resorts to destroying records he usually has conceded that management will discover the theft and the purpose of destroying the records is to prevent management from finding out who the thief is.

EXPENSE REIMBURSEMENT SCHEMES

Employees may falsify information about their business expenses and so cause their employers to compensate them in the form of inflated expense reimbursements. Sales people (and any person who is in a position to incur travel and entertainment expense) most commonly perpetrate this type of fraud by overstating or creating fictitious expenses in areas such as client entertainment and business travel. There are four general categories:

Mischaracterized expense reimbursements – Here the employee claims personal expenses or an expense that was legitimately made on behalf of the organization, but which falls outside the guidelines of the organisation's policy for reimbursement. Fraudsters submit receipts from their personal expenses and fabricate business reasons for the costs. Based on the false expense report the victim organization issues a cheque to the perpetrator. A common element of these schemes is the lack of detailed expense reports or any expense reports at all. Requiring detailed information means more than just supporting documents; it should mean precise statements of what was purchased, why, when, and where. These schemes are often regarded as 'fibs' and prevention efforts are not always taken seriously. In many organizations this sort of fraud is winked at and is considered a sort of fringe benefit that is an unofficial 'perk' of certain jobs.

Overstated expense reimbursements – There are 4 main schemes:

- ***Altered Support*** **-** Some employees exaggerate the cost of their business expenses to obtain a larger cash reimbursement. Employees can doctor receipts to reflect higher costs by using Tipp-Ex, ballpoint pens, typewriters etc. the fraudster may discard the actual receipt and fabricate fake one. If originals are not required the employee can attach a photocopy on which alterations will be less noticeable.

- ***Over purchasing*** – These schemes generally involve travel expenses. As an example, an employee buys 2 tickets for the same trip, one more expensive than the other. The employee submits the expensive receipt for reimbursement but travels on the cheaper ticket. The fraudster returns the expensive ticket for a refund and is reimbursed more than the flight cost. Merchandise returns are also often used to generate fraudulent reimbursements.

- ***Overstating another employee's expenses*** – Here the cashier who distributes expense reimbursements may overstate another employee's expenses. The cashier could alter the expense report, overstating the employee's expenses, and then distribute the correct amount to the employee while retaining the excess amount.

- ***Orders to overstate expenses*** – Here the employee and supervisor work in collusion. More commonly this scheme is used to channel money into a slush fund that is then used for bribes and gratuities that are paid to customers.

Fictitious expense reimbursements – Employees claim reimbursement for completely fictitious travel and entertainment expenses. Fictitious documentation often includes obtaining blank receipts from restaurants, hotels, airlines, or claiming expenses that were paid by others, as follows:.

- ***Producing fictitious receipts*** – Many employees manufacture their own fake support documents. Some 'cut & paste' receipts from legitimate suppliers, others may use calculator tapes, while others may use DTP equipment to create realistic-looking counterfeit receipts.

- ***Obtaining blank receipts from vendors*** – Employees sometimes obtain a stack of blank receipts from a vendor then use these to manufacture support for fraudulent expenses. If the receipts are consecutively numbered a red flag should be raised.

- ***Claiming expenses paid by others*** – Employees may seek reimbursement for expenses that were actually incurred, but which another person paid for, such as a business dinner.

Multiple reimbursements – Here several types of support are submitted for the same expense. Where organizations do not require original documents as support, employees could use several copies of the same receipt to generate multiple reimbursements, month after month. Employees could pay for the item with their credit card then submit the vendor's receipt and the credit card receipt as two different expense claims. Employees might also charge an item to the company credit card, save the receipt and attach it to an expense report as if they paid for the item themselves. The victim company then pays twice for the same item.

BILLING SCHEMES

Fraudulent disbursements are the most common form of asset misappropriation, and occur when an employee uses his position to cause payment for some inappropriate purpose. The most common and costly fraudulent disbursement is the billing scheme. Billing schemes attack the purchasing function of an organization and they cause the victim organization to buy goods or services that are nonexistent, overpriced, or not needed.

In a typical scheme, the fraudster creates false support for a fraudulent purchase. The fraudulent support documents, which can include invoices, purchase requisitions, delivery notes, etc., cause the victim organization to issue a cheque.

Employees can also utilize false billings to receive goods or services instead of cash. In these cases, the fraudster makes a personal purchase and charges it to his employer as if the purchase was a business expense.

The major categories of billing schemes are:

Shell company **–** these are fictitious entities created for the sole purpose of committing fraud. They are not really companies as they do not produce goods, supply services or occupy any physical space. The fraudster sets up his fictitious business as a 'vendor' to the victim organization. The employee then submits invoices from the shell company for fictitious goods or services.

Overbilling involving existing vendors **–** here the victim company is billed from a legitimate vendor for nonexistent or overpriced goods or services. There are 3 main methods:

- Kickback schemes where an employee works in collusion with an existing vendor. The vendor pays the employee to exercise his influence over the purchasing process.

- In Pay-and-return schemes an employee intentionally causes his employer to overpay a legitimate, non-accomplice vendor. This is achieved by paying an invoice twice, by paying the wrong vendor, or paying more than the invoice amount. The fraudster than contacts the vendor and asks that the excess payment amount be returned for his attention so the 'mistake' can be rectified.

- False invoicing from non-accomplice vendors. Here the fraudster either manufactures a fake 'existing vendor' invoice or re-runs an invoice that has already been paid. The employee submits the invoice and intercepts the resulting payment.

Personal purchases with company funds – Instead of cash, employees can purchase goods or services and bill them to their employers. Most fraudsters purchase personal items at their employers' expense by either running personal invoices through accounts payable or disguise the purpose of the expense as a business purchase, or they charge personal items on company credit accounts.

PAYROLL SCHEMES

Payroll schemes occur when an employee fraudulently generates over-compensation on his behalf. The most common forms of payroll fraud are:

Ghost employee schemes – a ghost employee is a real or fictitious person on the organisation's payroll who does not actually work for the organization. In this scheme, an employee falsifies personnel or payroll records that cause pay-cheques to be generated to a ghost. For the scheme to work, four things must happen: the ghost must be added to the payroll, timekeeping and wage rate information must be collected, a pay-cheque must be issued, and the cheque must be delivered to the fraudster.

Falsified hours and salary – For hourly employees, the size of the paycheque is based on two factors; the number of hours worked and the rate of pay. For an hourly employee to fraudulently increase his paycheque, that employee must either falsify the number of hours worked or change the wage rate. Timekeeping is generally done by time clocks, computers, or by manual timecards. Salaried employees would generate fraudulent salaries by increasing their rates of pay.

Commission schemes – Commission is a form of compensation calculated as a percentage of the amount of transactions a salesperson generates. A commissioned employee's wages are based on the amount of sales he generates and the percentage of those sales that he is to be paid. Therefore there are two ways the employee can fraudulently increase a paycheque – falsify the amount of sales made, or increase the rate of commission.

CHEQUE TAMPERING

Instead of relying on false support documentation to generate a fraudulent disbursement, the perpetrator of a cheque-tampering scheme takes physical control of a cheque and places false information on the cheque. The fraudster may forge a signature, alter a payee, alter the amount of the cheque or forge an endorsement.

Cheque tampering frauds depend upon factors such as access to the company cheque-stock, access to bank statements, and the ability to forge signatures and alter information on the face of the cheque. Cheque fraudsters commit fraud by identifying and exploiting weaknesses in an organisation's cheque payment system. The main methods of cheque tampering are:

Forged maker schemes – The person who signs a cheque is referred to as the 'maker' of the cheque. Here the employee misappropriates a cheque and then forges the authorized signatures. The employee would have to firstly get hold of a cheque. The fraudster could be an employee with access

to the cheque-stock (bookkeeper, finance manager, a/p clerk) or an employee without access to the cheques. In some organizations the cheques are left unattended, or the keys to the strongroom are left unattended, or the computer password is known to many people. The employee could also counterfeit a cheque if he cannot obtain an original cheque.

Forged endorsement schemes **–** Here the fraudster intercepts cheques after they have been signed but before they are mailed. The employee then forges an endorsement of the payee on the reverse of the cheque and banks the cheque into his or an accomplice's account. The employee could steal the cheques from the mailroom, or have the cheque posted to his box number.

Altered payee schemes **–** The employee steals a creditors or debtors cheque and then changes the payee name to his name, an accomplice's name, or to a fictitious company/individual. Obviously the fraudster could also change the amount. The details can be changed by mechanical erasure (razorblade), tipp-ex, adding additional payee details (trading as….) or the fraudster could enter the A/P system and change the names of payees before the cheques are prepared.

Concealed cheque schemes **–** The fraudster would prepare a cheque made out to himself, an accomplice, fictitious person, or with no payee designation. Instead of forging the signatures the employee conceals the cheque in a batch of legitimate cheques. The cheques are typically delivered to the signatories during a busy part of the day when he or she is not likely to pay close attention to them. False or old support documentation could be used.

Authorized maker schemes – The employee simply writes and signs the cheques as he would a legitimate cheque. Where company policy prohibits cheque signatories from handling blank cheques, the fraudster often uses his influence to overcome this control. The perpetrator will use his authority to deflect questions that may be raised. Intimidation can also play a large part in the commission and concealment of all types of occupational fraud.

In forged endorsement and altered payee schemes the fraudster steals a cheque intended for someone else. The major problem is that the legitimate payee most probably will complain when he does not receive payment. The fraudster will try to avoid this problem by causing the victim organization to issue a new cheque to the payee. This is achieved by forcing the computer to accept the same invoice number by adding a number or letter to avoid the duplicate check controls.

E. FRAUDULENT FINANCIAL STATEMENTS

Each year, unsuspecting investors shell out millions of dollars to companies whose financial health has been grossly misrepresented by its principals. According to the Association of Certified Fraud Examiners (ACFE), the average financial statement fraud scheme results in a $5,000,000 overstatement of assets or revenues and/or understatement of liabilities or expenses of a company.

SURVEY 1 - ACFE Report to the Nation
The ACFE is the recognized authoritative source for all types of information about fraud and white-collar crime. The Association's 'Report to the Nation on Occupational Fraud and Abuse' is the first study of its kind and is based solely on 2,608 cases over ten years. As a general rule, only more serious fraud and abuses are included. The Report is the largest known privately funded study on the subject. Fraudulent financial statements accounted for only 5% of offenses, but 64% of total losses in the ACFE's Report to the Nation!

Expanding on our previous definition of fraud, Financial Statement Fraud is:

> ***Deliberate fraud committed by management that injures investors and creditors through materially misleading financial statements.***
>
> Materiality = "The omission or misstatement of any accounting data or fact, which, when considered with all other information made available, would have altered the decision or judgment of the user."

Because financial statements are always the responsibility of management, Financial Statement Fraud is Management Fraud.

SURVEY 2 - Financial Mail BUSINESS ETHICS Survey - *14 July 2000:*
"HONESTY NOT THE BEST POLICY"
Most South Africans believe dishonesty is the route to business success…
That's one of the main findings in the Financial Mail's latest poll carried out by Ask Africa. Two hundred respondents were asked if they thought dishonest people tended to achieve financial success; 68% of male respondents and 51% of female respondents answered yes. On a language basis, 70% of Afrikaans-speakers, 57% of African-language speakers and 45% of English-speakers answered yes. The poll findings could suggest males and Afrikaans-speakers have a lower opinion of business ethics than other groups but, taken as a whole, the findings put business ethics in a poor light. This is confirmed by the rating of ethical standards of businesspeople in general: only 19% of males rated them high or very high, 49% males and 47% females rated them average and 32% males and 25% females low or very low.

SURVEY 3 - JOURNAL OF BUSINESS ETHICS Study:
Fraud remains one of the easiest and most lucrative crimes to commit. A study reported in the February 1996 *Journal of Business Ethics* found that 47 percent of senior executives, 41 percent of corporate controllers, and 76 percent of graduate business students were willing to commit securities fraud by failing to disclose write-offs that reduced corporate profits. Fourteen percent of executives, and 8 percent of controllers, were willing to actively inflate sales figures. To quote the cynical Raymond Chandler, these sad statistics suggest, ***"The difference between crime and business is that for business, you've got to have capital."***

SURVEY 4 - CFO Fraud Conference:
Attendees at an October 1998 conference sponsored by *CFO Magazine* were queried if they were ever asked to misrepresent their company's financial results. A good percentage (45%) had been asked, with 38% of the group complying. A whopping 78% had been asked to use accounting rules to cast results in a better light. Half of that group acceded to the request. A similar survey conducted at a *Business Week* CFO Conference found that 55 percent of the CFO's had been asked to misrepresent results. 17% complied with the request.

Requests to misrepresent earnings seem to be driven by company's desires to meet Wall Street expectations. This resulted in a number of companies committing financial statement fraud and using very aggressive accounting practices to enhance and "smooth" earnings. Earnings management becomes fraud when companies intentionally provide materially misstated information.

In response the SEC has taken numerous steps, including establishing an earnings management task force of 15 accountants within its corporate finance division. In December 1998 the task force began poring over financial documents to ferret out accounting irregularities - specifically, companies that manipulate earnings figures, improperly recognize revenues and misuse reserves are being targeted.

SURVEY 5 - COSO Report on Fraudulent Financial Reporting:
The Committee of Sponsoring Organizations (COSO) of the Treadway Commission sponsored the study, Fraudulent Financial Reporting: 1987-1997. This study is a comprehensive analysis of fraudulent financial reporting occurrences investigated by the SEC (Securities & Exchange Commission) from 1987 to 1997. Findings of the study can be grouped into five categories describing the nature of the companies involved, the nature of the control environment, the nature of the frauds, issues related to the external auditor, and the consequences to the company and the individuals allegedly involved.

Nature of Companies Involved

- ***Relative to public registrants, companies committing financial statement fraud were relatively small. Most of these companies had assets less than $100 million and were neither listed on the New York or American Stock Exchanges.***
- Some companies committing the fraud were experiencing net losses or were in close to break-even positions in periods before the fraud. Pressures of financial strain or distress may have provided incentives for fraudulent activities for some companies. Some companies were experiencing downward trends in net income in periods preceding the first fraud period, while other companies were experiencing upward trends in net income. Thus, the subsequent frauds may have been designed to reverse downward spirals for some companies and to preserve upward trends for others.

Nature of the Control Environment

- ***Top senior executives were frequently involved. In 72% of the cases the chief executive officer was involved and in 43% the chief financial officer was associated with the financial statement fraud. Other individuals also named in several cases included controllers, chief operating officers, other senior vice presidents, and board members.***
- Most of the audit committees only met about once a year or the company had no audit committee. Further most audit committee members did not appear to be certified in accounting or have current or prior work experience in key accounting or finance positions.

- Boards of directors were dominated by insiders and "gray" directors with significant equity ownership and apparently little experience serving as directors of other companies. Collectively the directors and officers owned nearly one-third of the company's stock.
- Family relationships among directors and/or officers were fairly common, as were individuals who apparently had significant power. In nearly 40% of the companies, the proxy provided evidence of family relationships among the directors and/or officers. The founder and current CEO were the same person or the original CEO/president was still in place in nearly half of the companies.

Nature of the Frauds

- Cumulative amounts of frauds were relatively large in light of the relatively small sizes of the companies involved. ***The average financial statement misstatement or misappropriation of assets was $25 million.***
- Most frauds were not isolated to a single fiscal period. Most frauds overlapped at least two fiscal periods, frequently involving both quarterly and annual financial statements. The average fraud period extended over 24 months.
- Typical financial statement fraud techniques involved the overstatement of revenues and assets. ***Over half the frauds involved overstating revenues by recording revenues prematurely or fictitiously***. Many of those revenue frauds only affected transactions recorded at period end. About half the frauds also involved overstating the value of inventory, property, plant and equipment and other tangible assets, and recording assets that did not exist.

Issues Related to the External Auditor

- All sizes of audit firms were associated with companies committing financial statement frauds. A Big Five (now only Big Four) auditor audited 56% of the sample fraud companies during the fraud period, and non-Big Five (now only Big Four) auditors audited 44%.
- All types of audit reports were issued during the fraud period. ***A majority of the audit reports issued in the last year of the fraud period contained unqualified opinions***.
- The study also found financial statement fraud occasionally implicated external auditors. Auditors were explicitly named in 29% of the cases. They were named for either alleged involvement in the fraud or for negligent auditing.
- Over 25% of the company's changed auditors during the time frame with the last clean financial statement period and ending with the last fraud financial statement period.

Consequences for the Company and Individuals Involved

- Consequences of financial statement fraud to the company often include bankruptcy, significant changes in ownership, and delisting by national exchanges, in addition to financial penalties imposed. Individual senior executives were subject to class actions legal suits and SEC actions that resulted in financial penalties to the executives personally. A significant number of individuals were terminated or were forced to resign from their executive positions. However, relatively few individuals explicitly admitted guilt or eventually served prison sentences.

Impact on Audit Committees and their Changing Role

As part of the SEC's ongoing assault on accounting irregularities, audit committees have come under intense scrutiny for not providing the independent oversight of a company's financial controls and reports that investors expect. Audit committee actions have also been questioned in the press. Some company's audit committee didn't review the work of the outside auditors for three years, while other company's audit committees met only once or twice per year. The audit committee plays a very important role, along with the financial director and the auditor, in achieving high quality internal financial controls and financial reporting by public companies.

The auditor has an obligation under professional literature to communicate with the audit committee or, lacking an audit committee, to those who have responsibility for oversight of the financial reporting process.

SEC Reaction

Chairman of the SEC, Arthur Levitt, discussed financial statement fraud and earnings management before the NYU Center for Law and Business on September 28, 1998. Chairman Levitt sees earnings management as a game among market participants. Specifically, he feels the motivation to meet Wall Street earnings expectations may be overriding common sense business practices. He spoke that too many corporate managers, auditors, and analyst are participants in a game of nods and winks. The Association of Certified Fraud Examiners, and Chairman Levitt, identified five specific practices (or schemes) used by companies to manage earnings:

- Timing differences
- Fictitious revenues
- Concealed liabilities and expenses
- Improper asset valuation
- Improper disclosures

TIMING DIFFERENCES

Timing differences are the recording of revenues and/or expenses in improper periods. According to GAAP (generally accepted accounting principles), revenues and corresponding expenses should be recorded or matched in the same accounting period. A company can enhance or lessen its profitability by choosing when it records revenues and expenses. Management use the following two methods to fraudulently record revenues and expenses in incorrect periods

- Early revenue recognition
- Recording expenses in the wrong period.

Early revenue recognition occurs when the company records a sale on the books regardless of meeting the criteria for the recognizing revenue. This makes the current-year financial statements look healthier and cheats the following period out of the sale. Recognizing revenues prematurely can involve the following: -

- Recording revenues when services are still due – according to the definition of revenue recognition, the services must be performed or the goods shipped before the sale can be recorded. Companies will often record a sale upon receipt of the cash even though the services have not been rendered. According to GAAP, when cash is received from a customer and some obligation remains, a liability should be recognized and once the services are performed, then the liability is reversed and revenue is recognized.

- Shipping goods before the sale is finalized – companies with income below expectations often rely on this scheme to boost revenues by shipping goods to clients before the delivery dates and often before the sale has taken place. Upon shipment the revenues are recognized prematurely.

- Holding the books open – involves advancing future sales into the current accounting period. This scheme allows a company to prematurely recognize revenue in one accounting period and then complete the sale in the next period. This scheme usually occurs at the end of a quarter or year.

Recording expenses in the wrong period – companies generally use this timing difference scheme to manipulate net income into an income overstatement to meet budget projections and investor expectations as well as a company's lack of accounting controls. There are two ways in which a company can record its expenses in the improper accounting period –

- Delayed expense recognition - the company shifts current expenses to a later accounting period by capitalizing revenue expenditures or by depreciating or amortizing costs too slowly. Capital expenditures are costs that provide a benefit to a company over more than one accounting period. These expenditures are depreciated over the asset's useful life. To make net income look healthier, a company may capitalize as many items as it can, thus pushing the expense into future periods. Fraud occurs when a company capitalizes items that are revenue expenditures. A company can also manipulate the useful life of an asset to falsify its earnings. Companies slowly depreciate their assets because the longer the depreciation period the less expense is recognized resulting in higher earnings. This stretched out depreciation also keeps the asset on the balance sheet longer, resulting in higher net worth. Intangible assets recognize the periodic cost expiration through amortization, a form of depreciation, and are manipulated by management in the same way as depreciation of capital assets.

- Premature expense recognition – the company shifts future expenses to the current accounting period by accelerating expenses into the current period, writing off future years' depreciation or amortization, or expensing capital expenditures. Management generally recognizes expenses prematurely to reduce the company's tax liability, push expenses into an already troubled period in order to make the next period look better, or record expenses in accounting periods in which income projections have been met. This allows companies to artificially show financial improvements in future periods. Writing off future years' depreciation is done by simply reducing the useful life of an asset, and so more expense is recognized thus resulting in a reduction of earnings. Expensing capital expenditures is done by not spreading the cost of an item over several periods, but expensing it in its entirety immediately – this reduces earnings in the current period but it increases subsequent period earnings because the depreciation expense is not recognized.

FICTITIOUS REVENUES

Fictitious revenues involve the recording of sales that did not occur. This scheme involves the creation or manipulation of transactions to enhance reported earnings. Management that wants their company to model a solid and financially sound operation will often resort to one of the following methods to create or inflate sales:

- Fabricating revenue
- Inadequate provisions for sales and returns
- Sales with conditions

Revenue fabrication - is used by management to create or manipulate a sales transaction for the sole purpose of producing fictitious revenues. This scheme often involves management creating fake or 'ghost' customers who make fake purchases. Artificial sales can also involve legitimate customers – a phony sales invoice can be generated for a legitimate client, or a legitimate client's order can be altered to reflect higher prices or quantities sold. Management could also use their own funds to purchase goods thereby giving the illusion of high sales volumes. They could also sell fictitious products or ship products for which customers are not obligated to pay.

Companies that create fictitious revenues tend to reverse the sales in the following period with a credit. By crediting the sale in the next period the company can create the sales it needs to meet its projected quarter or year-end figures, then simply remove the sale at the start of the next quarter or after the books are closed for the year.

Inadequate provisions for sales and returns – when a company makes a sale there is always the possibility that the goods will be returned by the buyer, therefore the company establishes an allowance for returns. In addition, the purchaser may be allowed a price reduction because of defects or for other reasons. Here the company would report a sales allowance. Both allowances are estimated by management and recorded at the time of the sale. The account 'allowances for sales and returns' reduces the initially recorded sales figures therefore it is located on the income statement as a contra account to sales. This 'offset' account informs the readers of the financial statements that not all the revenue recorded on the statements will be recognized. Fraud is perpetrated when the company does not record the sales return or allowance on its books. This accounting technique artificially overstates revenues.

Sales with conditions - are sales that have not yet been completed and the risks and rewards of ownership have not passed to the purchaser. The most common examples are conditional sales and consignment sales. Conditional sales are sales that are contingent upon certain events occurring in the future, such as client acceptance of a product or the seller's performance of certain acts outlined in the sales agreement. Companies with aggressive revenue recognition policies record conditional sales regardless that the customer is under no commitment to buy and the title of risk and loss remains with the seller.

Goods on consignment are also not considered sales as the consignor delivers these goods to an agent, the consignee, who tries to resell the goods. The consignor retains the title of the goods and the risk of loss until the agent sells the goods.

CONCEALED LIABILITIES AND EXPENSES

Liabilities represent the obligations that a company has to creditors. Normally, readers of financial statements tend to look unfavourably at companies with significant amounts of debt – therefore management often tries to conceal the debt. When liabilities are kept off the books the company's equity, assets and/or net earnings are fraudulently inflated. Management uses the following schemes to conceal expenses and liabilities:

- **Liability/expense omission** – Fraud is perpetrated in the liabilities section of the balance sheet by either understating liabilities or failing to record liabilities. Typically, when a company omits its liabilities, the related expenses are also omitted, resulting in the net income being falsely overstated. The schemes used by management to fraudulently omit liabilities and expenses are failing to record liabilities either partially or entirely, reporting revenue rather than a liability when cash is received for goods or services that have not yet been performed by the seller, and failure to record contingencies, like litigation and guarantees.
- **Omission of warranty and product liability** – Companies often grant customers a warranty on a product and these warranty costs should be recognized at the same time the revenue is recorded. By not recording the warranty liability, a company is understating its liabilities and overstating its net income. A product liability is a liability that results from selling defective products to clients. If a company is aware that one of its products is defective it should establish a product liability but companies can face product liabilities so great that they are

forced into bankruptcy due to their insolvency caused by the publicity of the product faults. Companies therefore want to conceal the product liability, for the time being, to avoid potential financial disaster and lawsuits.

IMPROPER ASSET VALUATION

Generally, the more assets a company can show on its books, the better the company looks to investors. Companies use assets to make more money and to pay off debts. Improper asset valuations take the form of one of the following classifications:

- **Inventory** – by definition, inventory excludes long-term assets subject to depreciation accounting. Inventory is tangible property – finished goods or work in progress. Improper inventory valuation is commonly done by improperly estimating obsolete, slow-moving goods (by not writing down inventory to reflect the proper asset value a company can overstate its inventory and increase its net earnings by mismatching revenues with cost of goods sold), fictitious inventory & the manipulation of count sheets (a company shows inventory on its financial statements that does not exist or is improperly valued), failure to record the purchase of inventory (a company inflates its earnings by not recording the inventory or the related expense upon the sale of the goods), and improper inventory capitalization (a company can inflate its inventory by shifting costs, such as fixed overheads, from the income statement to the balance sheet).

- **Accounts receivable** – are regularly falsified and manipulated in much the same manner as revenue and inventory and these schemes often work side-by-side with each other. 'Fictitious receivables' and 'failure to write down accounts receivable for bad debts' are the two most commonly used schemes. Fictitious accounts receivable is prevalent in companies with financial difficulties and whose managers receive commissions based on sales. Management tends to create fictitious accounts receivable at the end of the year in order to overstate sales. Almost all companies have accounts receivables that are uncollectible and GAAP requires that these receivables be written down to their net realizable value, which is the amount of cash the company expects to collect in the future. Management should establish a reserve called an allowance for uncollectible accounts. Management estimates how much of its credit sales will not be collected and then it recognizes an expense for this uncollectible amount called bad debt expense. By manipulating the allowance for doubtful accounts management can alter the financial statement in two ways; the value of the accounts receivable is overstated, and net income is overstated due to the bad debt understatement.

- **Fixed assets** – are frequently manipulated by management booking fictitious fixed assets (recording fixed assets that are not legally owned by the company), misrepresenting asset value (fixed asset costs are recorded above cost), improper capitalization (the cost of maintaining an asset is included in the asset value), and misclassification of assets (by falsely classifying long-term assets as current assets discharge its current obligations with its current assets – in its favour).

- **Business combinations** – occur when two or more business entities combine their operations. There are two methods for accounting for business combinations: the purchase method (used when cash or other assets are distributed as a result of the combination or if the liabilities are incurred as a means of financing the purchase), and the pooling method (used when only shares are issued to effect the business combination).

IMPROPER DISCLOSURES

The principal of disclosure requires management to clearly and adequately report all material, relevant information regarding the economic affairs of a company in its financial statements. When a company withholds key information through improper disclosure, the readers of the financial statements are misled. The following items frequently receive improper disclosure by management:

- **Liability omissions** – these include failure to disclose loan covenants (agreements that are part of a financing arrangement) and loan defaults (defaulting on the loan agreement), and contingent liabilities (pending litigation, guarantees of indebtedness, & collectability of receivables) and commitments (long-term rental agreements).

- **Significant events** – these include recalls of products, new technology having an effect on sales, obsolescence of inventory, and any other significant event that. If not disclosed, would render misleading financial statements.

- **Management fraud** – Management has an obligation to disclose to the company's shareholders significant fraud committed by officers, executives, and others in positions of trust, by failing to disclose management fraud, the company preserves its integrity and escapes embarrassment at the expense of the shareholders.

- **Related-party transactions** – a related party is a party that has the ability to control or influence the other party in making financial and operating decisions. If the relationship is not disclosed, the financial statement reader will assume that the transaction is an independent, third party, arms-length transaction. Examples of related parties are companies with common directors, companies in partnership, a parent and subsidiary company, a common majority shareholder, and relatives. Not all related party transactions are fraudulent but actions like transferring liabilities to affiliates and overstating assets as amounts due from affiliates are.

- **Changes in accounting policy** – Information is more useful to readers of the financial statements if the data can be compared with other data from similar enterprises (comparability), or with information about the same company between different periods (consistency). A company that makes accounting changes to enhance its financial appearance but does not disclose the changes in its financial statements is in violation of GAAP and is misrepresenting information to investors and creditors. There are 3 types of accounting changes that should be disclosed – changes in estimates (service lives of assets, warranty liability and uncollectable accounts receivable), changes in accounting principles (change in depreciation methods and inventory methods), changes in the accounting entity (mergers and acquisitions, and selling subsidiaries)

The fundamental differences between fraudulent financial reporting *and the* misappropriation of assets:

CHARACTERISTIC	***FRAUDULENT FINANCIAL REPORTING***	***MISAPPROPRIATION OF ASSETS***
Definition	Intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users	Theft of an entity's assets
Perpetrator	Usually perpetrated by management	Usually perpetrated by employees; might be perpetrated by management
Who is harmed?	Third-party users of the financial statements	The entity
Who benefits?	The entity and perhaps the perpetrator(s), though indirectly and usually at some future point in time	The perpetrator — directly and immediately
Relevance of internal controls	Ineffective controls might indicate an inappropriate attitude regarding controls of the financial reporting process. Improper attitude might indicate a willingness to commit fraudulent financial reporting (indirect relationship between controls and the risk of fraud)	Ineffective controls provide an opportunity for misappropriation of assets (direct relationship between controls and the risk of fraud)
Likelihood of fraud being material to financial statements?	By definition, fraudulent financial reporting is meant to deceive third-party users. Therefore, it is almost always material; otherwise it wouldn't have its desired effect	Might or might not be material to the financial statements

Fraudulent financial reporting is a serious problem with serious consequences. The damages incurred by financial statement fraud are widespread, affecting not only investors and creditors, but auditors, employees and honest competitors, to name a few. No company is immune from fraudulent financial reporting. In fact, the possibility of fraud is simply inherent in doing business. However, the risk of its occurrence can be reduced provided sufficient attention is expended on the matter.

As you have learned, the responsibility for proper and reliable financial reporting rests with management. Top management is responsible for setting the tone and creating and maintaining a corporate environment dedicated to mitigating the incidence of financial statement fraud. The corporate environment should include an Audit Committee and an internal audit function, both of which should be effective and informed.

Although each of these entities' roles enhances the propriety and reliability of the financial reporting process, occasionally there are weaknesses in this corporate structure, which allows for fraudulent financial reporting to be committed. The auditing procedures and other techniques presented in this training course should be used in the event these weaknesses do occur. Although the techniques and procedures discussed in the course are general, they should provide you with a basic understanding and foundation for preventing and detecting financial statement fraud.

Stepped up enforcement activities targeting fraudulent and aggressive accounting policies, companies' obligation to comply with Corporate Governance codes, and a shift in liabilities from banks to companies, make it incumbent on the internal auditor to assess these risks to the organization.

Financial Statement Analysis

Financial statement analysis is a process enabling readers of the financial statements to develop and answer questions regarding the financial data presented. A variety of financial analysis techniques utilized to examine unexpected relationships in financial information often are referred to as analytical techniques or procedures. Analytical procedures are based on the premise that relatively stable relationships exist among economic events in the financial statements in the absence of known conditions to the contrary. The amounts represented in the financial statements reflect the economic events and will be relatively stable. Contrary conditions that cause stable relationships to not exist might include unusual or nonrecurring transactions or events; accounting, environmental, technological changes; errors, illegal acts, or fraud. Therefore, deviations in expected relationships might signal fraudulent reporting, thus warranting investigation of the deviation. An analytical procedure is the study of interrelationships and trends in financial, operating, and other data for the purpose of identifying accounts that are misstated.

Analytical procedures are used to detect and examine relationships of financial information that do not appear reasonable. They are useful in identifying:

- Differences that are not expected
- The absence of differences when they are expected
- Potential errors
- Potential fraud and illegal acts

Comparative Techniques

The following techniques are commonly employed by an examiner to identify the relationships among the financial data that do not appear reasonable.

- *Comparison of current period information with similar information from prior periods*. Prior period amounts normally are assumed to be the expectation for the current period. A modification of this comparison is the incremental approach whereby prior period numbers are adjusted for known changes such as significant purchases or sales of assets and changes in lines and volumes of business.

- *Comparison of current period information with budget or forecasts*. Include management's expectations for unusual transactions and events.

- *Study of relationships among elements of information*. Certain accounts vary in relation to others, both within a financial statement and across financial statements. For instance, commissions are expected to vary directly in relation to sales.

- *Study of relationships of financial information with the appropriate non-financial information*. Non-financial measures are normally generated from an outside source. An example would include retail stores where sales are expected to vary with the number of square feet of shelf space.

- *Comparison of information with similar information from the industry in which the organization*

operates. Industry averages are reliable in stable industries. Unfortunately, industry trade associations require months to compile, analyze and publish information; therefore, the data may not be timely.

- *Comparison of information with similar information from other organizational units.* A company with several stores might compare one store with another store. The "model" store should be sufficiently audited to provide assurance that it is an appropriate standard.

Unexpected Relationships

When analytical procedures uncover an unexpected relationship among financial data, the examiner must investigate the results. The evaluation of the results should include inquiries and additional procedures. Before inquiring of the company's employees and management as to the variations, an examiner should first establish expectations for the causes of the variances. An examiner equipped with his own interpretations of the variance will be better suited to ask meaningful questions when interviewing company personnel. Explanations derived from employees should be tested through examination of supporting evidence. For example, if the sales manager indicates that the increase in sales is due to a new advertising campaign, examine the advertising expense account to verify that the campaign did occur. If the advertising expense is similar to the prior year, where there was no advertising campaign, the relationship is not reasonable and fraud may exist.

Financial Relationships

In order to identify relationships that appear unusual, an understanding of general relationships between certain financial statement balances is necessary. If sales increase, how should cost of sales respond? If commission expense decreases, what would be expected of sales? Answers to question such as these are the foundation of financial analysis. The following relationships are general, and traditionally occur between financial accounts; however, unique circumstances may render different results.

- *Sales vs. Sales Returns and Discounts*
  Whenever a company sells merchandise, there is the possibility that it will be returned. Customers are not always satisfied with their purchases and goods can be defective. The greater the sales, the greater the chance of returned merchandise. The relationship, therefore, is directly proportional. This also is true for sales discounts. If a company offers its customers a discount on its purchases, then more sales equal more potential discounts.

- *Sales vs. Cost of Goods Sold*
  The company generates sales because it sells its merchandise. This merchandise had to be purchased, manufactured, or both; all of which entail a cash outlay for materials, labor, etc. Therefore, for each sale, there must be a cost associated with it. If sales increase, then the cost of goods sold generally increases proportionally. Of course there are cases where a company has adopted a more efficient method of producing goods, thus reducing its costs, but there still are costs associated with the sales that are recognized upon the sale of the goods.

- *Sales vs. Accounts Receivable*
  When a company makes a sale to a customer, the company generally ships the merchandise to the customer before the customer pays, resulting in an accounts receivable for the company. Therefore, the relationship between the sales and the accounts receivable is directly proportional. If sales increase, then accounts receivable should increase at the same rate.

- *Sales vs. Inventory*
  A company's inventory is merchandise that is ready to be sold. A company generally tries to anticipate future sales, and in doing so, tries to meet these demands by having an adequate supply of inventory. Therefore, inventory usually reflects the growth in sales. If sales increase, then inventory should increase to meet the demands of sales. Inventory that grows at a faster pace than sales might indicate obsolete, slow-moving merchandise or overstated inventory.

TYPES OF ANALYTICAL PROCEDURES AND INTERPRETATIONS

Auditors and financial statement examiners employ several techniques to manipulate plain, unconnected numbers into solid, informative data that is instrumental in interpreting the company's financial standing. Creating relationships between numbers offers more insight into the financial well-being of an organization. By comparing these relationships with other industries or businesses within the same industry, an examiner can extrapolate viable evidential matter and have a greater comprehension of the company's financial condition.

There are three principal types of analytical tests employed by examiners in analyzing financial statements and detecting fraudulent reporting – trend analysis, ratio analysis, and reasonableness tests. We will focus on trend analysis because it the easiest method to employ.

Trend Analysis

Trend analysis is the examination of the trend of the account balances as a basis for determining whether the current period data potentially are misstated, that is, whether they depart significantly from the trend of the prior data. Trend techniques vary from the very simplest of manners such as two-period comparisons to the more complex statistically based time-series models. Two categories of analysis that focus on the trends of the financial accounts are called horizontal and vertical analysis.

- *Horizontal Analysis* is a technique employed to analyze the percentage change in individual financial statement items from one year to the next. The first period is considered the base period, and the changes to subsequent periods are computed as a percentage of the base period. As an example, if net sales are R250,000 in 1997 and R450,000 in 1998, the percentage change would be 80%.

  An important consideration to note when utilizing this analytical technique is to incorporate a material rand amount into the analysis. For instance, if an account is R1,000 in 1997 and R2,000 in 1998 this percentage increase is 100%; however, the rand amount is only R1,000. For most companies a R1, 000 change is immaterial and warrants very little attention. On the other hand, if the account increased only 5% but the rand amount is a R50,000,000 change from the prior year; such an amount would be of considerable interest to the auditor.

- *Vertical Analysis* is a technique that analyzes the relationships between the items on an income statement, balance sheet, or statement of cash flows by expressing components as percentages. For instance, all income statement components are a percent of net sales and all balance sheet components are a percent of total assets on the asset side and as a percent of total liabilities and equity on the liability and equity side. Net sales, total assets and total liabilities & equity are assigned 100%. For example: Cash/Total Assets = XX%, or Salaries/Net Sales = XX%. The relationships are then compared from period to period.

F. ORGANISED CRIME

Professional and Amateur Criminals

Much economic street crime is caused by occasional criminals. Their decision to steal is largely related to opportunity, and these thefts are neither well-planned nor well- executed. In addition, included in this group of amateurs, are the millions of occasional thieves who earn their incomes legitimately, but engage in such activities as shoplifting, pilfering, and tax fraud. These crimes are believed to be caused by situational inducement or opportunity. Because the perpetrators are not professional offenders, it is believed that they respond best to the general deterrent effect of the law.

Occasional property crimes occur when there is an opportunity or situational inducement to commit crime. Opportunities are available to all members of all classes, but members of the upper class have more opportunity to engage in lucrative business-related crimes.

Professional thieves make the bulk of their income from law violations. Most are not deterred by the law, and many are very skilled at their craft. Not a great deal is known about the professional thief except that three types of offenders can be identified. One group is young people who are taught the craft of theft by older professionals; another is gang members who continue their thieving after maturing out of gang activity; and the third category includes youths who are incarcerated for minor offences and learn the techniques of professional theft while in prison.

Commercial Thieves

Commercial thieves can be categorized into two categories: burglars and hijackers. The main goal Of the burglar is to acquire cash. Some commercial thieves burglarize establishments that favour Cash rather than credit card businesses. Examples include supermarkets, bars, and restaurants. They frequently work in teams and spend a great deal of time and effort planning their heists.

Hijackers specialize in stealing goods in transit from trucks, trains, and other commercial carriers. Their targets are selected because they contain large quantities of goods that are usually less secure than merchandise in warehouses. In general, commercial thieves do not specialize in one kind of merchandise but rather pick the best opportunity. There are several theories on the causes of commercial thievery.

Organized Crime

Historically, organized crime has been regarded as a law and order problem confined to single states or cities, for example geographic areas, such as southern Italy and Sicily, and cities, such as Boston or Hong Kong. However, more recently, assisted by developments in technology and the reality of the 'global village', the nature of organized crime has expanded its interest to become a transnational phenomenon. In reality, organized crime is a business that, like any legitimate business, is concerned to reduce risks, maximize profits and diversify by crossing borders.

Organized crime is a conspiratorial activity, involving the coordination of many people in the planning and execution of illegal activity or in the pursuit of a legitimate activity through unlawful means (for example, using threats in order to secure a stake in a legitimate corporation). Organized crime involves continuous commitment by primary members, although individuals with specialized skills (such as contract killers) might be brought in when the need arises. Organized crime organizations usually are structured along hierarchical lines – a chieftain supported by close advisors, and then lower echelon members.

Organized crime has economic gain as its primary goal, though achievement of power and status also

might be a motivating factor. Organized crime is not limited to providing illicit services. It includes such sophisticated activities as laundering illegal money through legitimate business, land fraud, and computer crimes. Most organized crime income comes from narcotics distribution, loan sharking, and prostitution. However, billions of dollars are gained from white-collar crime, gambling, theft rings, pornography, and other illegal enterprises.

Alien *Conspiracies*

The *alien conspiracy theory,* adhered to by the government and many respected criminologists, holds that organized crime is a direct offshoot of the Mafia. A major premise of the alien conspiracy theory is that the Mafia is centrally coordinated by a national committee that settles disputes, dictates policy, and assigns territory. Not all criminologists support this theory. Some believe organized crime is made up of ethnically diverse groups who compete for profits and territory.

According to the alien conspiracy theory, organized crime is comprised of a national syndicate of *26* Italian-dominated crime families who call themselves La Cosa Nostra. The major families have a total membership of about 1,700 “made men” and another 17,000 or so “associates” who are criminally involved with syndicate members. The families are controlled by a supposed “Commission” made up of the heads of the five New York families in addition to bosses from Detroit, Tampa, Boston, Buffalo, and Chicago, who settle personal problems and enforce rules that allow members to gain huge profits through the manufacture and sale of illegal goods and services.

Some scholars charge that the traditional view of organized crime and the Mafia is fanciful. They argue that the alien conspiracy theory has been too heavily influenced by media accounts of the testimony of one person, mobster Joseph Valachi, before an U.S. investigation headed by Senator John McClellan. Valachi’s description was seized upon by conspiracy theorists as an accurate portrayal of mob activities. Critics challenge its authenticity. For example, criminologist Jay Albanese compared Valachi’s statements with those of another mob informer, Jimmy Fratianno, and found major discrepancies with respect to the location and extent of organized Crime activity.

Alan Block’s work is at the heart of the argument by critics that a tightly controlled and organized mob does not exist. Block argues that independent crime organizations can be classified as-one-of two kinds: *enterprise syndicates or power syndicates.* The former are involved in providing illicit services through madams, drug distributors, bookmakers and the like. The latter perform no task except to terrorize. Through coercion, buy-outs, and similar means, power syndicates graft themselves onto enterprise systems, legal businesses, and trade unions.

While the problem of organized crime is easily sensationalized, there is a widely held perception that South Africa – a society particularly vulnerable because of its state of transition, weak border controls and sophisticated banking networks – is fast becoming the target of overseas crime syndicates. With Western Europe and America tightening the screws on international crime syndicates, notably drug traffickers, they have been forced to divert their attention elsewhere which may explain why South Africa has become a favourable candidate for infiltration. Tentative estimates by the South African Police Service (SAPS) suggest that there are currently between 200 and 500 "*extremely well financed and superbly armed*" crime syndicates operating in and from South Africa, with almost half of these operations based in and around Johannesburg.

These highly sophisticated criminal organisations know how to exploit the freedom of movement of capital, financial services, goods and persons. Operations include a lucrative trade in drugs, gold and diamond smuggling, vehicle theft, commercial crime and arms smuggling. The activities of these

various organized crime networks are often closely linked. In Southern Africa, for example, vehicle theft and robbery are linked to the illegal arms trade in Mozambique, while drug trafficking is connected with motor vehicle theft and money laundering in Zambia. Economic crime, in particular, is highly attractive to syndicates that regard it as a high-reward, low-risk activity that is often employed to protect 'core' criminal activities. As such, any attempts to combat organized crime syndicates will involve preventing commercial crime.

While varying in form and structure, organized crime operations in South Africa, as elsewhere in the world, share a number of common characteristics:

- Organized crime is comprised of participants who incorporate themselves into more or less complex systems for the purpose of committing crimes. These systems have a hierarchy of control, with clearly designated ranks and systems of promotion and payment;

- The second attribute of organized crime is its instrumental nature. Instrumental crimes are defined as illegal acts committed when individuals unable to obtain desired goods and services through conventional means, resort to crimes-for-profit. Organized crime, at its core, offers illegal goods and services in order to make profits -- examples are illegal gambling, prostitution, pornography, loan-sharking, bootlegging, and fees for "protection" in the form of extortion. Organized crime has also been known to promote other crimes-for-profit, such as bank robbery, hijacking, labor racketeering, burglary and arson. Organized crime exists for the sole purpose of making money.

- The use of weapons to ensure that 'business' routes are protected and potential competitors eliminated. Murders within the world of organized crime are generally committed to ensure the ongoing survival and profitability of the organization;

- Sophisticated procedures, often *via* legitimate business interests, to launder money obtained by illegal activities; and

- The fifth common trait of organized crime is the ability to penetrate and use the institutions of state. Good state contacts enable operations to run more smoothly, while forewarning crime bosses of any impending government crackdown. In some countries, such as Colombia and Russia, it is often difficult to tell where the state ends and organized crime begins. Crime syndicates have the ability to 'buy into' government and bribe officials – including those in law enforcement – who earn comparatively little. While it is well known that bribery occurs in the lower ranks of the SAPS, the degree to which the higher echelons of the service may have been penetrated is unclear.

- Political corruption (*graft*) is a critical part of the survival of the business of organized crime. Note that graft generally falls into one of two categories: ***clean*** or ***dirty:***
  Clean graft is comprised of payoffs that allow organized crime members to run certain non-violent and so-called "victimless" rackets, such bookmaking, prostitution rings and labor racketeering. Clean graft also comes in the form of payments for forgiveness of minor transgressions such as traffic/parking tickets.
  Dirty graft is money offered to cover up murder, rape, armed robbery or drug trafficking. It should be understood that most law enforcement officials would not accept "dirty graft." The line between clean and dirty graft is, however, illusory -- clean graft ensures the survival of the "victimless" rackets that, in turn, fund more serious crimes, such as murder for hire and drug

trafficking.

- The last distinguishing attribute of organized crime is its generational persistence -- criminal organizations such as Mafia crime families continue to operate despite fluctuations in membership. While the death or retirement of family bosses and other leadership figures can result in significant changes, it does not cause individual crime families to cease to exist.

  The generational persistence of organized crime can be attributed in part to an auxiliary feature common to all crime syndicates: rules of conduct. The survival of any organization is dependent upon the predictable and orderly conduct of its members. A set of rules, or "code," establishes obedience and predictable conduct, and a set of established sanctions for violations ensures continued adherence and obedience.

In recent years, RICO statutes and increased vigilance on the part of law enforcement agencies have significantly weakened the American Mafia. The Mafia's adaptive nature, however, ensures that while it may be down, it will never be out. Although many of its bosses are in prison and several of its more lucrative extortion schemes have been broken up, **the Mafia has adapted by shifting to white-collar crime**. Its deeply entrenched and pervasive powers of corruption extend well beyond the "traditional" mob activities such as extortion and drug trafficking, and into nearly every facet of legitimate business. The Mafia owns waste management companies, construction firms, is firmly seated on Wall Street, runs several fraud schemes involving cheques, credit cards, EFT’s ... the list is endless.

It is the adaptive nature of organized crime that is both its most important defining characteristic, and the one that ensures its survival. It is the flexible and persistent nature of the American Mafia, in conjunction with the characteristics listed above, that have enabled its evolution from loosely knit bands of extortionists around the turn of the century to a high-tech, multinational conglomerate.

According to comparative research on the growth of organized crime elsewhere in the world, South Africans should be aware of and monitor the following trends:

- The changing commodities that organized crime networks trade in and potential new commodities they may seek to obtain;

- The dynamic connections between various syndicates, street level operations, and linkages to the state and external criminal operations; and

- The changing shape and structure of organized crime syndicates in reaction to some forms of policing and specific targeting of police agencies, either to be corrupted or for violent retribution.

The increased sophistication and growth of organized crime also partly result from new communications technology that has opened up new areas of criminality in the commercial world, as well as new opportunities for laundering money or investing profits from illicit activities. In the process, the distinction between legal and illegal sectors of any economy become blurred and the most 'respectable' organized crime operations are often a dynamic mix between legal and illegal activities.

H. COMPUTER CRIME – THE NEW THREAT

Willie Sutton, the famous bank robber, was once asked why he robbed banks. His answer was: ***"Because that's where the money is".*** That's no longer true of course as there is far more money transferred electronically now than was ever held in bank vaults.

EFT's are used by banks to move more than $1 trillion in funds around the globe each day and the amount is rising. Because of the large volume processed through EFT systems, they are a prime target for fraud perpetrators wanting an immediate, enormous source of money.

Therefore, EFT systems are high risk and should receive the highest priority for security measures. As these FBI statistics show, more dollars change hands with EFT's than any other method but only make up a slight percentage of total transactions:

Transactions		
Category	Number	Dollars
Cash	80 percent	5 percent
Cheque	18 percent	12 percent
EFT	2 percent	83 percent

The volume of EFTs continues to grow as more companies use this medium to conduct business yet 83% of Americans use cheques as a payment method and it's estimated that cheques will continue to be used as the most favoured payment method well into the low to mid 2000's.

Why? - Of the 70 billion cheques issued in the USA in 2000, 500 million were defrauded (-1%);
- Paper is easier to trace and leaves an audit trail;
- More interest is earned on cheques that are delayed;
- The R amounts on fraudulent incidents are much greater with electronic transfers; and
- Currently there is less liability for companies using cheques than using electronic transactions;
- The dilemma is that while computers are needed, they are not trusted.

While EFT losses or near losses are seldom admitted, they do occur. Here are four tales that have circulated privately among bankers and consultants courtesy of EFT consultant Richard Bort:

- One large corporation that used EFT extensively would routinely deliver a magnetic tape loaded with multiple wire instructions every day. The company was supposed to apply a unique identifier to the tape box, and the bank was supposed to inspect it to make sure the tape was authentic, but the procedure became so routine that the tape authentication drill was relaxed. That mistake almost proved fatal when an insider slipped a bogus wire instruction onto a bogus tape and the bank accepted and executed the tape, including a bogus wire directing a large amount of money to a private off-shore bank account. An alert banker up the chain from the bank where the wire was initiated caught it just before the funds would have left the country.

- In another incident EFT instructions were authenticated by call-back — someone in the bank's EFT room would pick up the phone and call the authorized corporate official to confirm that a wire request the bank received was indeed authentic. Culprits inside the company used automatic

call forwarding to bypass the real authority and divert the calls to someone who was in on the scheme and would approve the fraudulent wires. Once again, it got past the initial bank and was caught further up the line before the funds left the country. "The call-back is a flawed security technique because the banker doesn't really know whom he is talking to," Bort reflects. Nevertheless, thousands of companies still use it today.

- A third near-loss was perpetrated by a consultant who had been working in a large bank for months and had stolen the internal codes used by bank personnel to authorize EFT's. He also had found out which accounts had high balances and almost no activity. One day he called the bank's EFT room, gave the proper code to identify himself as a branch officer of the bank and directed $10 million to his own Swiss bank account. The transfer took place. The man even withdrew some of the money to buy several diamonds. But the theft was detected, the man was arrested before he could leave the country, and nearly all of the money was recovered.

- Organized crime groups are using the Internet for major fraud and theft activities. Perhaps the most notable example of this occurred in October 2000 and concerned the Bank of Sicily. A group of about 20 people, some of whom were connected to mafia families, working with an insider, created a digital clone of the bank's online component. The group then planned to use this to divert about $400 million allocated by the European Union to regional projects in Sicily. The money was to be laundered through various financial institutions, including the Vatican bank and banks in Switzerland and Portugal. The scheme was foiled when one member of the group informed the authorities. Nevertheless, it revealed very clearly that organized crime sees enormous opportunities for profit stemming from the growth of electronic banking and electronic commerce.

"$1 Billion in $100 bills is 15 cubic yards, $1 Billion in gold weighs 80 tons, $1 Billion in E-Cash is 32 bits - surely a prescription for fraud on a breathtaking scale?"
- Dr Bob Blakely

The old saying of "Use a thief to catch a thief" is true to a certain extent, but the interpretation of this statement is that in order to prevent abuse we have to start to understand and think like the criminal. In so doing we can start to identify the areas of risk that are being capitalised on.

For many businesses, the threat of computers or cybercrime is not even a consideration as their primary business does not involve any 'on-line' trading, so they believe they are not at risk. This cannot be further from the truth, as the fact that you even have a computer in the workplace qualifies you to becoming a victim irrespective of how the fraud or crime is to be perpetrated. In a report issued by the Department of Trade and Industry in the UK in 2002, attacks by hackers on firms tripled in the past two years and 80% of companies have fallen victim to hackers, viruses or fraud.

The most serious losses were caused by theft of proprietary information and financial fraud, which begs the questions as to the value you placed on your data!

Typical examples of computer crime are (1) Hackers (2) E-theft - stealing of money via electronic transactions (transferring money to own bank a/c) (3) Netspionage - confidential information stolen by hackers, to sell to a competitor/ use to exploit another business (4) Domain Name Renewal Scams (5) Telecom fraud - accessing a company's telephone exchange and via using a computer program permits calls to be resold to other users and (7) Identity Theft / Phishing - utilizing other people's identity (credit card info, identity numbers, etc) to make unauthorized purchases

THERE ARE PRIMARILY FOUR GENERAL COMPUTER CRIME TYPES:

- **Computer as the target:**
  Crimes in which the computer is the target include such offenses as theft of intellectual property, theft of marketing information, or blackmail based on information gained from computerized files. It could also entail sabotage of intellectual property, marketing, pricing, or personnel data, or sabotage of operating systems and programs with the intent to impede a business or create chaos in a business' operations.

  Techno-vandalism occurs when unauthorised access to a computer, results in damage to files or programs, not so much for profit but for the challenge. Techno-trespass occurs when someone is 'walking' through a computer just to explore.

  In all of these crimes, the offender uses the computer to obtain information or to damage operating programs. The crime is committed by 'superzapping' or by becoming a 'super user'.

  It's easy for individuals experienced in computer operations, to become a 'super user' because virtually every system has a trap door. Trap doors permit access to systems should a problem either a human or technological one arise. This then gives the intruder access to nearly every file in the system.

- **Computer as the instrumentality of the crime:**
  An instrument to facilitate committing a crime. The processes of the computer, not the contents of computer files, facilitate the crime.

  The criminal introduces a new code (programming instructions) to manipulate the computers analytical processes, thereby facilitating the crime. Another method involves converting legitimate computer processes for illegitimate purposes.

- **Computer is incidental to other crimes:**
  The computer is not essential for the crime to occur, but it is related to the criminal act. The crime could occur without the technology, however computerization helps the crime to occur faster, permits processing of greater amounts of information, and makes the crime more difficult to identify and trace e.g. money laundering.

  All of these situations require unique data recovery techniques in order to gain access to the evidence.

- **Crimes associated with the prevalence of computers:**
  The presence of computers and notably the widespread growth of microcomputer's, generates new versions of fairly traditional crimes. Technological growth essentially creates new crime targets e.g. black-market computer equipment and programs, violation of copyright restrictions of commercial software, etc. The potential loss to businesses can be quite staggering.

By identifying the type of attack and asking questions like…

- Could we be subject to any of the above?
- Would this form of attack be identified?
- What would the consequences be if the attack were successful?

… You can then decide what security is necessary.

The Computer Security Institute offers the following checklist:

- *Password security*: In computing environments that allow reusable passwords, ensure that strong passwords are chosen. Insist that passwords contain an alphanumeric mix and are at least six to eight characters long. If appropriate, use third-party software to enforce password composition rules and forced password changes. Alternately, consider implementing one-time passwords or tokens for authentication and authorisation.
- *Anti-virus defence*: Install anti-virus software at both the network server and workstation levels. Keep up with current versions and do not allow users to disable software. Use both a scanner to detect existing viruses and an activity trapdoor to look for hitherto unreported viruses.
- *Network communications*: Use encryption to protect sensitive data sent over networks.
- *Remote access*: For secure dial-in access, implement unique user Ids and passwords, limited access times and limited connection duration's. Consider token cards and dial-back modems.
- *Internet access*: Do not allow Internet access unless firewalls and other key components of information security are in place. Firewalls should not be your sole means of defense.
- *Mobile computers*: To secure mobile computers, install access control programs and physical security devices. Consider encryption and token cards.
- *Buy smart*: before purchase, evaluate products for security features. After purchase, disable default accounts and change default passwords. Turn on all appropriate audit and security features.
- *Audit*: Conduct regular and frequent reviews of security logs and audit trails. Institute an incident report procedure.
- *Identify risks*: Conduct a thorough risk analysis of your computing environment. If you don't have the expertise in-house, look for outside help.
- *Enforce policies*: Develop comprehensive policies and procedures for all aspects of information security, and make sure they are enforced.
- *Educate your users*: Raise the security awareness of your users with an enterprise-wide educational campaign. Warn them about social engineering. User-oriented computer security newsletters, videos and posters can also be effective tools. Tell employees why security controls are necessary and teach them how to use them.
- *Educate yourself*: There is a wide range of training, conferences, books, periodicals and newsletters on computer security.

10 Data security tips from the FBI's NCCS:

- Disable all system default accounts, or change default passwords shipped with systems.
- Do not display company banners, online help, or other enticements before a user is authenticated. In other words, know whom you are dealing with prior to providing them with information.

- Disable network services that provide valuable information that a hacker could use to exploit system security.
- Do not allow users to log directly into a host as root. Users should log in their own Id's to root.
- Password composition should discourage password cracking (e.g. dictionary attacks) or guessing a password. Third-party software should be used, if necessary, to administer composition rules. Simply put, passwords should contain both alpha and numeric characters and be six to eight characters in length.
- Limit the number of invalid login attempts a user is permitted to discourage password guessing.
- Record security violations and review security logs.
- Use encryption to protect sensitive information transmitted over a network.
- Install up-to-date system patches that correct security weaknesses exploited by hackers (e.g. sendmail vulnerabilities).
- Discourage the use of trusted relationships where trust is not warranted. For example, limit the use of files that would allow a user to access a host without providing a password.

Six basic Gateways into the Payment System

1. Submission of forged payment instruction by letter, phone, etc
2. Seek assistance of junior bank employee
3. Enter company or bank premises under the guise of an external contractor
4. Via bribery or intimidation, gain co-operation of Bank employees to transfer funds
5. Via bribery or intimidation, gain co-operation of Company employees to transfer funds
6. Hack into Bank or Company network (brute-force or social engineering)

Selective Computer Crime Timeline

- 1973 A teller at New York's Dime Savings Bank uses a computer to embezzle over $2 million.
- 1978 Security Pacific National Bank is hit by a $10.2 million computer fraud.
- 1981 Wells Fargo Bank suffers a $21.3 million hit from computer fraud.
- 1986 Prudential Bache (London, UK) – 51 year old Angelo Lamberti transfers $8 million.
- 1988 Kevin Mitnick, America's most famous hacker, is accused of causing $4 million damage to government computer systems and stealing $1 million worth of software.
- 1988 First National Bank of Chicago is victimized in a $70 million computer heist.
- 1990 A Bulgarian research institute releases 24 previously unknown computer viruses.
- 1990 An Australian hacker closes down NASA computers after penetrating their system.
- 1992 Evidence is produced of industrial espionage in Australia relating to the bugging of several large companies' fax lines.
- 1994 A 16-year-old student nicknamed Data Stream is arrested by London police for penetrating computers at the Korean Atomic Research Institute, NASA & several US government agencies.
- 1994 Five members of the Aum Shinri Kyo cult's Ministry of Intelligence break into Mitsubishi Heavy Industry's mainframe and steal megabytes of sensitive data.
- 1995 A French student cracks Netscape's encryption system used for commercial transactions.
- 1995 A Russian hacker, Vladimir Levin, illegally transferred over $10 million from Citibank to private accounts using a laptop computer.
- 1995 A Japanese bank employee was arrested for using a PC to steal 140 million yen.
- 1996 Bell Research Laboratories in the US are able to counterfeit smart cards.
- 1996 High School student called Koki infiltrated one of S.A.'s top 4 bank's computer systems.
- 1997 America On-line (AOL), one of the largest Internet service providers in the US, cuts direct access for its users in Russia due to a "daunting level of fraud."

- 1997 The Times of London reported that several multinational banks, anxious to maintain public confidence, paid millions of pounds hush money to hackers to keep quiet their successful intrusions into the banks' networks
- 1997 In a demonstration on German television the Chaos Computer Club of Hamburg wrote a program that allowed hackers to transfer money from other people's bank accounts to their own.
- 1998 A hacker stole 48 000 encrypted passwords from companies around the world and used an Internet program called "John the Ripper" to decode the encrypted passwords.
- 1998 The information age has hit Botswana with a bang: government and the private sector have gone on-line and the largest Internet service provider has just reported the first hack attack.
- 1999 Two brothers from China's Jiangsu Province were sentenced to death for breaking into a bank computer system and transferring money into their own accounts.
- 1999 - the Pretoria web site, SA Police Services, TELKOM, and many others were hacked.
- 2000 Hackers broke into Microsoft Corp.'s computer network and stole blueprints to the latest versions of the company's Windows and Office software.
- 2001 Hackers stole the credit card details of, among others, Microsoft boss Bill Gates, billionaire George Soros, advertising tycoon Martin Sorrell, & Palestinian leader Yasser Arafat.
- 2001 Nigerian man hacked into South African and international financial institution's internet databases and transferred hundreds of millions.
- 2002 DBSA's and SARB's web sites are 'spoofed' by a Nigerian crime syndicate.
- 2003 ABSA receives a lot of bad press re the e-blaster 'hacker'
- 2004…ChildPorn and Spyware attacks more prominent
- 2005 Various SA Banks (reportedly Standard Bank and FNB) had their sites spoofed and their 'identity' was stolen; ABSA experience a 'employment opportunity' scam where posts for over 600 people was advertised

Effective preventative measures are much cheaper and far less painful than post-fraud investigation and litigation".

Peter Rossof, Treasury Director, AT&T

I. REDUCING YOUR FRAUD RISK – Prevention

The best method of avoiding fraud is to stop it before it occurs. To do so, controls and alertness must be created at all levels within the organisation. Care must be taken, however, to avoid creating an atmosphere of distrust and paranoia by over-emphasizing fraud deterrence.

If audit is to contribute to the prevention and detection of fraud it is essential that auditors understand how to build programs that address this goal. Effective awareness programs and internal controls can help prevent crimes of opportunity. Employees not tempted by weak or non-existent controls, and not encouraged by poor management practices, are less likely to commit frauds.

There is an ironic side to good internal controls that you should be aware of. The successful prevention of fraud – or the lack of symptoms – may leave some organisations overly complacent. It is easy to forget the negative affects of fraud when you are not experiencing them. Therefore the value of prevention programs is never more widely agreed upon than when such programs are allowed to erode, frauds occur, and are eventually detected. The prompt detection of fraud then reaffirms the need for prevention programs. However, a failure to detect fraud will be seen (perhaps unfairly, if controls were allowed to lapse) as a significant shortcoming. But until this happens, the company finds itself in the position of wondering ***'is no news good news – or not?'*** The onus is on internal audit and management to remain vigilant and maintain the controls. No news *is* good news provided controls are enforced and regularly reviewed.

FRAUD HEALTH 'CHECK-UPS'

We have found that in many organisations there is an over-reliance on traditional techniques for fraud prevention and detection. These techniques are often performed by individuals who do not have a wide exposure to the many types of fraud threats facing an organisation. Research indicates that the majority of frauds are still discovered by chance rather than through detailed procedures.

Traditional risk reviews are useful exercises but, by themselves, are limited because reviews based on individual company knowledge often fail to identify problems (and solutions) that have occurred elsewhere, & the reviewers tend to fixate on their area of specialty so 'leaving many stones unturned'. Thus, internal/external risk assessments performed by external specialists are essential in order to provide a satisfactory solution to protect an organisation's profits and reputation.

Document Security Review

There are two keys to effective document security assessment. One is the Potential Value at Risk and the second is the Environment in which the transaction will be completed. There are essentially two types of transaction environments: CONTROLLED and UNCONTROLLED. Items like gift vouchers or event tickets are normally transacted in a controlled environment. In the controlled environment staff may be trained to spot key features of a document to authenticate it very quickly. In the uncontrolled environment it is virtually impossible to train or educate all the people transacting the documents.

Uncontrolled environments are typical of cheque cashing locations. There are no uniform standards for acceptance of a cheque in payment or cheque cashing. Anyone willing to accept a cheque may do so. Education is an enormous task and is going to take time and money. The big question is, "Who will do it?"

Once we know what environment we are dealing with, we may next examine the potential for loss. If the document in question has a potential value of one rand, it would make no sense to pay for extensive security features. However, if the document is routinely transacted for several thousand rand, effective security features now become crucial. (All rules are out when a company is a victim of fraud, and cost becomes far less an issue).

We must now remember, as in the one rand example, it matters little when a low value, single document is defrauded. But what if you could redeem thousands of one rand documents? How much is security worth now? You can see that there are no firm procedures for this exercise. Procedures should be personalised for each end user situation.

Risk Assessment looks at:

- What may go wrong,
- The areas in the organisation that may be most vulnerable to fraud,
- The likelihood of fraud occurring, and
- The possible impact if it does occur.

Risk Management then looks at what could and should be done about these fraud risks.

There are 6 good reasons for every organization to have fraud prevention Health Check-Ups:

1. **It could save your organization.** Fraud can be a catastrophic risk. If you don't proactively identify and manage your fraud risks, they could put you out of business almost overnight. Even if you survive a major fraud, it can damage your reputation so badly that you can no longer succeed independently.

2. **It could pinpoint opportunities to save you a lot of money.** Fraud is an expensive drain on an organization's financial resources. In today's globally competitive environment, no one can afford to throw away the estimated 6% of revenues that represents the largely hidden cost of fraud. If an organization isn't identifying and tackling its fraud risks, it is disadvantaged against competitors who lower their costs by doing so.

3. **Fraud is now a common risk that shouldn't be ignored.** The incidence of fraud is now so common that its occurrence is no longer remarkable, only its scale. Any organization that fails to protect itself appropriately from fraud should expect to become a victim of fraud, or rather, should expect to discover that it is a victim of fraud.

4. **It's the least expensive way to find out the organization's vulnerability to fraud.** Most organizations score very poorly in initial fraud prevention check-ups because they don't have appropriate anti-fraud controls in place. By finding this out early, they have a chance to fix the problem before becoming a victim of a major fraud. It's like finding out you have seriously high blood pressure. It may be bad news, but not finding out can be a lot worse.

5. **It's a great opportunity for an organization to establish a relationship with a Certified Fraud Examiner on whom they can call when fraud questions arise**. Since the risk of fraud can be managed but is rarely eliminated, it's likely that the organization will experience fraud in future and will need a CFE's assistance.

6. **A strong fraud prevention program could help increase the confidence** investors, regulators, audit committee members and the general public have in the integrity & quality of the organization's financial reports. It could also help to attract and retain capital.

A fraud prevention 'check-up' provides owners, senior managers or those charged with governance, with valuable insights into major gaps in an organisation's fraud prevention measures. Like an annual physical from a doctor, it's a wise precaution that may save you from an unexpected peril.

"Fraud is like cancer. Most of us know someone who has it. We know people who will eventually have it. It has become common but we can take steps to protect ourselves through healthy choices and regular check-ups using the latest tools and technology. But if people ignore the problem and live dangerously then there's a much greater chance of becoming a victim."

-Toby Bishop, CEO of the Association of Certified Fraud Examiners

The King II report urges organisations (both private and public) to establish systems that identify risks early & continuously and then to establish internal controls to mitigate the risks.

In the USA, many states require that organizations have a formal fraud prevention program. Also, more and more clients are insisting that you have a fraud prevention & detection program before they will even consider doing business with you. It's in all stakeholders' interests to ensure there is little or no fraud, as fraud losses tend to be made-up on product prices, therefore affecting everyone right down to the consumer.

A formal **fraud prevention and detection program** is now fast becoming one of the most important **competitive advantages**, and companies that don't have one run the very real risk of losing a lot of business - sales and marketing directors take note!

For those organizations that state they don't have fraud, Business Against Crime has this to say: ***"100% of all businesses in S.A. are affected by fraud. It is only the extent of this crime that differs from company to company".*** BAC goes further to say ""In contemporary South Africa it is more likely that the opposite is true, for such is the scale of commercial crime that there are no organisations that are not affected, and an organisation with a clean internal crime record is itself liable to speculation that it is soft on crime and therefore not protective of shareholders interests".

FRAUD PREVENTION: A FOUR-STEP APPROACH

…as recommended by Courtenay Thompson & Associates:

1. ***SCREEN OUT FRAUDSTERS BEFORE HIRING THEM***
2. ***REDUCE OPPORTUNITIES FOR FRAUD***
3. ***CREATE AN 'ANTI-FRAUD' ENVIRONMENT***
4. ***PROSECUTE ALL FRAUDSTERS***

The four-step approach to fraud prevention is based upon the reduction of opportunity and incentive. Research studies and experience show that opportunity and likelihood of being detected play major roles in the individual decision to commit fraud.

1. ***Screen out those who are likely to commit fraud.*** The organization can:

   - Do criminal background checks on employees and vendors, in accordance with law.
   - Call previous employers to verify employment dates.
   - Confirm school transcripts, degrees, and certifications.
   - Consider checking credit history for applicants in high exposure areas.
   - Consider drug testing.
   - Consider psychological testing.

2. ***Reduce the opportunity for fraud.*** Managers can:

   - Be sure your internal control decisions include considerations of what kinds of fraud can be perpetrated, and by whom.
   - Be sure that subordinates, in making decisions about controls, are fully aware of the fraud implications of the controls that suggested or already in place.
   - In areas where segregation of duties is not practical, use alternative controls to reduce opportunity. Management sampling of work and quality assurance techniques have proven valuable.

3. ***Create an environment in which employees believe that dishonest acts will be detected*** by management, monitoring techniques, other employees, and the auditors.

   - Bring fraud into the open. Discussion of implications of internal controls, and review of frauds reported in the newspapers and journals heighten awareness.
   - Consider conducting an in-house Program for supervisors and managers covering dishonest and fraudulent activities that can occur, and what the symptoms might be.
   - Determine that the fraud implications of controls designed & intended to detect fraud are fully understood by the responsible clerical & supervisory personnel.
   - Establish communication methods that encourage employees to report suspected fraud directly to those responsible for investigation without fear of disclosure or retribution.
   - Consider the use of a fraud hotline, if appropriate, for the reporting of suspected fraud.

4. ***Create an environment in which dishonest acts are not tolerated and are punished***.

   - Develop and implement a policy for handling suspected dishonest and fraudulent activities, including termination and reporting to law enforcement.
   - Communicate such policy to all employees, agents, vendors, contractors, and other interested parties.
   - Develop and implement a code of ethics for employees, clearly defining acceptable and unacceptable activities.

- Develop and implement codes, guidelines, and organizational policies designed to prohibit conflicts of interest. Consider requiring employees to disclose possible conflicts of interest involving other employees.

- Require all vendors and contractors to agree in writing as apart of the contract process, to abide by the codes described in points above.

Simply put, fraud can be proactively managed by:

- Creating a fraud awareness culture
- Ensuring that you have appropriate guardians in your business
- Be involved and understand what controls are in place
- Review and monitor with an element of surprise
- Reward compliance
- Introduce controls and procedure certification
- Other actions:
  - employee rotation programs
  - employee leave policy
  - development of code of conduct/ethics, fraud / corruption control plan
  - review annual effectiveness of above-mentioned policies
  - vendor tender programs
  - consult annually with specialist to review your progress
  - consider formal whistleblower arrangements

"An Ounce of Prevention is Worth a Pound of Cure"

J. REDUCING FRAUD RISKS AT STAFF LEVEL

FRAUD PRONE PERSONALITY TYPES

What type of person commits fraud? More than 99% of employees are honest, trustworthy and loyal. There are early warning signs out there for the other less than 1% as long as we keep our eyes open. Some may seem obvious, others not so. Watch out for an employee who:

- Has a close relationship with a vendor or vendors, but is usually a loner
- Indicates a need to control operations, and have custody of assets
- Disregards segregation of duties, controls and procedures
- Frequently expresses discontent with their job
- Creates an adversarial relationship with auditors and other groups inside and outside the organisation
- Is reluctant to take vacations or be away from the office
- Lives an extravagant lifestyle or possesses expensive items not consistent with the position
- There are indicators of heavy personal debt or other personal problems
- Has frequent mood swings, significant changes in behaviour, compulsive tendencies

A person that commits fraud will probably exhibit more than one of the above behaviour patterns.

In their book 'Fraud Watch – a guide for business', Ian Huntington and David Davies of KPMG discuss the following four character sketches that illustrate some of the more common aspects of deceptive behaviour:

1. ***Successful Sam***
   - Boasts about having all the right contacts
   - Is over-optimistic about business prospects
   - Gives the impression of being wealthy & successful
   - Is entertained or entertains lavishly
   - Flatters people to get his own way
2. ***Eva the Deceiver***
   - Doesn't allow people to see the full picture
   - Says as little as possible & Passes the buck
   - Uses delaying tactics – always busy with something else
   - Answers different questions from the ones put to her
   - Goes on the attack when confronted with matters she doesn't want to discuss
3. ***Martin the Manipulator***
   - Manipulates deadlines and timetables behind closed doors
   - Exploits ignorance by blinding people with science
   - Carefully controls access to certain clients, suppliers or colleagues
   - Deals with certain accounts personally outside the main system
   - Plays one person off against the other
4. ***Conscientious Connie***
   - Never takes a long holiday
   - Seems very conscientious & tends to be a loner
   - Keeps people at arms length – very territorial
   - If unavoidably absent, ensures that all problems are left until her return

Note: *Please keep in mind that the above traits by themselves do not necessarily indicate fraud. They may however be the first indication that there could be fraud. A person that commits fraud will probably exhibit more than one of the above behaviour patterns for each character sketch.*

NOW, HOW WELL DO YOU KNOW YOUR EMPLOYEES?

- **Training** - Fraud Education and awareness of staff actively involved on a daily basis with issuing and reconciling cheques is crucial, as the most effective weapon against the criminal is each staff member's vigilance and knowledge. Regular training programs should ensure that all staff understand the security measures they are required to undertake.

- **Random spot checks** should be carried out and certain job functions should be randomly rotated.

- **Screen new employees carefully** - Application forms should be comprehensive and information verified. At least two references should be contacted directly. For sensitive positions the police recommend that applicants complete a security questionnaire followed by an interview with people skilled in security & interview techniques.

- **Be aware** of employees whose personality and work habits change. Remember that references do not always tell the whole story. Most embezzlers work alone and can be repeat offenders.

- **Encourage good employee relations** - If staff and management communicate, know each other well and feel part of a single team, there will be an in-built resistance to fraudulent acts. Such achievements cost little and have other benefits too.

- **Performance appraisals and counseling sessions** should be used to know and understand employees better and to look for motives, character changes or attitudes that might lead to fraud.

- **Encourage staff to be vigilant** - It is unlikely that fraudsters will be able to conceal their every move, and employees need to be positively encouraged to report any incident or circumstances that they think may compromise the organisation's security. There must also be clear channels for employees to go through and guarantees that nothing will be held against them even if their suspicions are mistaken. Anonymous toll-free hot-lines seem to be very effective in encouraging both insiders and outsiders to report their suspicions of fraud - even low-level fraudulent activities that may lead to much bigger frauds.

THE FRAUD TRIANGLE

There are hundreds of ways to perpetrate fraud, and there are three key elements common to all of them. The three ingredients are, (1) strong financial pressure, (2) a way to justify or rationalise the fraud as being OK, and (3) a perceived opportunity to commit & conceal the fraud.

Fraud examiners need to understand what motivates people to commit fraud and how fraudsters operate. Fraud results from a combination of opportunity, need/greed, and attitude/culture. The fraud examiner and management must be cognizant of what the motivations of fraud are and be able to assess what motivations would be more applicable in any particular case.

Fraud results from either a need or greed. Research has also shown that fraud motivated by need is highest when the economy is in a slump and fraud motivated by greed is highest when the economy is booming. The former because people may come on hard times and try to maintain their standard of living and the latter because in times of boom there is greater consumerism.

This need or greed however must have a combination of other factors such as the opportunity to commit the fraud and the attitude. The opportunity to commit the fraud results from the perpetrator having access to the assets at the point in time that the fraud is committed. This may be just temporary access; however access is needed to the asset. The opportunity to commit fraud usually results from a lack of proper internal controls.

The other factor can be called the culture of the organization. Organizations which expect unreasonable performance standards, have little respect for controls, are not sensitized as to how serious fraud is, allow an employee to rationalize that it's OK to do the deed etc. tend to have a higher incidence of fraud.

Opportunity is the most controllable factor followed by the culture. In many organizations, however, management, in most cases, does not take the necessary steps to control these factors.

In many ways fraud is like fire. In order for a fire to occur, three elements are necessary: 1. Heat, Oxygen, & Fuel, and when these three come together there is a fire. As with the elements in the fire triangle, the three elements in the **Fraud Triangle** are interactive. With fire, the more flammable fuel, the less oxygen and heat it takes to ignite. Similarly, the purer the oxygen, the less flammable the fuel needs to be to ignite. With fraud, the greater the perceived opportunity or the more intense the

pressure, the less rationalization it takes to motivate a person to commit fraud. Likewise, the more dishonest a person is, the less opportunity and/or pressures it takes to motivate fraud.

Pressures that motivate individuals to commit fraud are as follows:

- Financial pressures
- Vices (drugs, gambling, alcohol)
- Work-related pressures, and
- Other pressures (nagging spouse or a challenge)

"Gambling was the ultimate experience for me – better than sex, better than any drug. I had withdrawal tortures just like a heroin junkie". "I degraded myself in every way possible. I embezzled from my own company – I even conned my six-year-old out of his pocket money".

"I was branch manager of a large bank. But secretly I was shooting up in my office each day and stealing money from the bank to buy drugs". "There was no level to which I wouldn't descend in order to get drugs. While I was a supposedly successful businessman, I shoplifted, broke into homes & stole anything that would bring cash to support my habit".

Opportunities

Opportunity, the first key ingredient, exists because of autonomy and ineffective procedures to ensure people's work is checked or monitored. Employees who know that their work is not checked may see the opportunity to commit fraud. Opportunity also stems from a poor organisational culture or ineffective distant leadership. Opportunities increase if there are poor physical and financial controls over assets, but still exist even if controls are good. Opportunities are provided by:

- A weak internal control environment
- Lack of internal control procedures
- Failure to enforce internal controls, and
- Various other factors such as apathy, ignorance, lack of punishment etc.

Rationalisations / Absence of Guardians

Rationalisation refers to the manner in which people think about their work, performance, contribution, etc within the workplace – often a perception of how they view themselves. Based on this view, they attach a value that they should derive from the company for being productive or delivering something of value, etc. Rationalisations that are commonly used by fraudsters are:

- 'The organisation owes it to me',
- 'I am only borrowing the money',
- 'Nobody will get hurt',
- 'I was keeping up with my hero',
- I was overlooked for promotion several times',
- 'The pay here is so bad we all have to supplement our incomes – everybody does it',
- 'I deserve more',
- Referral fees are common in this industry',
- 'It's for a good cause', or
- 'It's either my integrity or my reputation'

Absence of guardians refers to the situation where there are limited or no processes in the organisation to test the integrity of the financial information or processes. The absence of the

integrity process includes an absence or ineffective role of internal auditors, external auditors, Board of Directors, Reporting requirements – banks, regulators, etc and appropriate management review.

The fraud triangle consists of three motivating factors that encourage fraud. This training course covers tried and tested methods of preventing fraud by creating a culture of honesty, openness, and assistance and by eliminating fraud opportunities. The risks of fraud can be reduced to very low levels if all stakeholders in an organisation are motivated to do so. The primary focus of the training course is Fraud Prevention, where big savings for an organisation can occur, and Fraud Detection, which is rarely done on a proactive basis. Fraud investigation, which costs million of Rands in South Africa every year, should be conducted on a much more efficient and effective basis.

Factors that help reduce 1 or more Fraud Triangle elements:

PRESSURE**:**

- Avoid setting unachievable financial goals
- Have a positive work environment
- Eliminate external pressures that may tempt management to prepare fraudulent financial statements
- Remove operational obstacles blocking effective financial performance such as working capital restraints, excess production volume, or inventory restraints
- Establish clear and uniform accounting procedures with no exception clauses
- Adopt an Employee Assistance Program (EAP). EAP's offer a range of counselling referral services dealing with substance abuse, mental health, family problems, crisis help, legal matters, health education, retirement, career paths, job loss troubles, family financial planning, etc.
- Establish "hotlines" for anonymous reporting of ethical problems and instances of fraud. The most effective kind of hotline arrangement is to have a third-party hotline co-ordinator.

RATIONALISATION**:**

- Management's philosophy and operating style significantly influence the company's consciousness in terms of committing fraudulent behaviour. By establishing policies and procedures that emphasize the importance of maintaining reliable accounting records, employees are more likely to incorporate these matters in the performance of their duties. An individual will be less likely to commit fraud in an organization that strictly enforces & strongly encourages compliance with policies & procedures.
- ***Written ethical standards should be established.*** An organization's ethical standards bring awareness and understanding of its requirements and expectations to its employees. The values of the company should be codified in a company's ethics policy or code of conduct.
- ***Employees should receive adequate training.*** Training is an important tool that organizations have to translate the written standards into reality. Training is the key to creating and maintaining a corporate culture. Training reinforces the rationale for having standards of ethical conduct and explains to employees the underlying structures, rules and procedures and how they function

within the culture of the organization. Training ensures that employees are aware of the provisions outlined in the written ethical standards.

- ***Managers should set an example by promoting honesty in the accounting area.*** It is important that management practice what they preach. Dishonest acts by management, even if they are directed at someone outside the organization, create a dishonest environment that can spread to other business activities and other employees.
- ***Honest and dishonest behaviour should be defined in company policies.*** Defined accounting policies should clear up any grey areas in accounting procedures.
- The consequences of violating the rules and the punishment of violators should be clear.
- Try to hire honest people

OPPORTUNITY**:**

Establish an Internal Control System

In most cases of fraud the opportunity to commit and conceal the deceitful act was feasible because the internal control structure that existed, if at all, was weak and not utilized to its capacity. A strong, effective internal control structure, when operating according to its capabilities, will assist greatly in the deterrence of fraud. Management is responsible for the components of the company's internal control structure. Management establishes the control environment, assessing the risks of the organization, identifying the information and communication channels and content, especially for its accounting system, designs and implements activities and monitors the controls. The objectives of an internal control system should be to:

- Encourage *adherence* to management's prescribed policies and procedures
- Promote *efficiency* in all of the firm's operations
- *Safeguard* assets of the company
- Assure *accuracy* and *reliability* of the accounting data and information

The ***first three objectives*** are concerned with the *operational system.* In essence, their purposes are to achieve operating effectiveness and operating efficiency, and provide adequate security for the company's assets. The internal controls are established to ensure:

- Functions are adequately segregated
- All transactions are executed in accordance with management's general or specific authorization
- Adequate physical control is maintained over assets and accounting records

The ***last objective***, which focuses on accuracy and reliability of accounting data, is related to the *transaction processing system.* The following objectives should be fulfilled in order for a company to

ensure that its accounting data is accurate and reliable.

- Transactions entered for processing are valid and authorized.
- Valid transactions are captured and entered for processing on a timely basis.
- Input data of all entered transactions are accurate & complete, & transactions are expressed in proper monetary values.
- All entered transactions are processed properly to update all affected records.
- All outputs, such as financial statements, are prepared by appropriate rules from complete, up-to date records in accordance with GAAP.

Create and Maintain a Control Environment That Exhibits Zero Tolerance for Fraud

An enterprise's control environment significantly influences the manner in which the financial statements are prepared and the internal control structure is established and maintained. A strong control environment typically reflects the effort and commitment on behalf of management in their effort to detect and prevent fraud. Although a strong control environment does not guarantee that fraudulent financial reporting will not occur, it does, however, significantly reduce the likelihood that management will manipulate the numbers.

Prepare Budgets and Perform Planning Practices

Budgets often are vital in detecting fraud, thus reducing the perceived opportunity. A company's financial objectives are founded in budgets. Budgets establish the revenue levels the company expects to achieve and the expense levels it hopes to restrain. By analyzing the variances between the actual amounts vs. the budgeted amounts, one can possibly detect and deter fraudulent activity through investigating the differences, identifying the causes and developing controls to prevent them in the future.

- Maintain accurate and complete internal accounting records.
- Monitor the business transactions and interpersonal relationships of suppliers, buyers, purchasing agents, sales representatives and others who interface in the transactions between financial units.
- Establish a physical security system to secure company assets, including finished goods, cash, capital equipment, tools and other valuable items.
- Discourage collusion by rotating staff and ensuring that annual leave is taken.
- Communicate policies to all stakeholders – we have found that if an employee asks for a kickback, the supplier may assume that it is the organisation's unwritten policy. An ethics policy will leave no doubt that the employee is acting without the organization's blessing and the supplier may report the incident to management.
- Proactive fraud auditing – this simply means that the auditor looks for fraud instead of waiting until fraud is reported. Auditors must be skeptical at all times.

"Don't put Dracula in charge of the blood bank!"

ETHICS

Why should a person be required to study ethics? There are 4 reasons for studying ethics:

1. ***People do not know what is ethical*** unless they study it. Ethics are not inherited. People do not automatically know how to make ethical decisions. Most of us fail to recognize when a decision has a moral component and we often overlook the moral consequences of our decisions.

2. ***Ethics provide an essential foundation for business transactions.*** Our system is based on a foundation of trust and honesty. Although many transactions are governed by written contracts and legal restrictions, the vast majority of our business transactions are made between parties who trust each other. Countless transactions are made by phone calls and letters between people who have never seen each other face-to-face or shaken hands.

3. ***Ethics are essential for organizational effectiveness.*** Unless employees believe organizational decisions are fair and just, they will not be willing to exert the effort and commitment necessary for the organization to succeed. This is derived from the idea that people need to know that what they are doing is socially meaningful and worthwhile.

4. ***Ethics are necessary for interpersonal relationships***—as it is for organizational success. Friendships depend on integrity. People do not like to associate with people they cannot trust. Honesty and trust are usually the most highly prized personal attributes, regardless of whether the respondents are asked to describe spouses, friends, coworkers, supervisors, neighbors, or politicians.

Some people claim that the moral foundations for deciding right and wrong are formed in childhood before the age of six or eight and nothing in later life significantly changes this moral foundation. While most moral values are learned in early life, there are several good reasons why people should continue to study ethics as adults:

- Moral behavior includes both knowing what to do and deciding to do it.
- Our commitment to choose the right is not fixed in childhood, but continues to develop (or weaken) throughout our life.
- Studying ethics helps to strengthen our resolve to behave ethically.
- Many of the moral issues we face in our adult lives are different than the issues we faced as children. Unless we continue to study ethics, we will not recognize these ethical issues or know how to respond to them.

Morality versus ethics

Moral does not always mean the same thing as ethical. Technically, there is a difference between saying something is immoral versus saying it is unethical.

- ***Ethics are usually defined by a written code of ethics.*** Many organizations and professions have written codes of ethics. Behavior that conforms with these standards is considered ethical. Conversely, behavior that violates a written standard is unethical. Therefore, it would be unethical for health care professionals to publicly discuss their patients' private information since this violates the confidentiality standards in their codes of ethics. An action is ethical if it is consistent with the stated requirements in a code of ethics. (The words ethical and moral are often used synonymously because some standards of conduct are universally accepted even though they are not written).

- ***To say an action is immoral means that it is wrong or harmful.*** Anything that is not just or fair, or that unnecessarily harms people and society, is immoral. There are many things that are immoral that may not be unethical because they do not violate a written standard in a code of ethics. (Integrity is a personal attribute characterized by being true at all times to high moral principles and having attitudes and behaviors that are consistent with these principles).

- ***Most people, however, do not make such a narrow distinction between morality and ethics.*** They do not require an act to violate a written code of ethics to be considered unethical. The justification here is that some behaviors are so generally regarded as right or wrong that they need not be written. The general consensus that they are always wrong is sufficient to equate immoral with unethical. Therefore, most people think that to say something is immoral is also to say it is unethical.

- ***Five ethical principles can be derived from philosophical writings.*** These five principles represent the basic criteria for making moral decisions. They are not equally relevant for all moral issues, nor do they always produce consistent conclusions. Nevertheless, they represent important criteria that ought to be considered in analyzing a moral dilemma and normally all five criteria should be considered.

- The five criteria are summarized here. The first two criteria are derived from teleology (Teleology is one of two major approaches for deciding right and wrong. According to teleology, right is defined by the ends or moral consequences of an action. An action is moral if it produces desirable consequences) and the next three from deontology (Deontology is the second of two major approaches to deciding right and wrong. Deontology comes from a Greek word meaning “ought” and is defined by duties and obligations. While teleology examines the consequences of an action to see if they are desirable, deontology examines the processes to determine whether they are fair and consistent with one's moral obligations).

  1. **Egoism and economic self-interest.** The argument here is that we are all expected to protect our own self-interests without interfering with the rights of others. This principle applies to individuals acting on their own as well as to groups of individuals acting for an organization.

     Actions that are not profitable usually cannot be sustained. Therefore, the principle is “never take any action that is not in the long-term best interest of yourself or the organization you represent.”

2. **Utilitarianism.** Since morality is defined in part by the consequences of an action, one way to decide whether an act is moral is to examine its consequences. Moral actions are expected to create the greatest good for the greatest number of people. This moral criterion, called utilitarianism, focuses on maximizing the benefits to society with the least amount of harm.

   The principle is "never take any action that does not result in greater good than harm for society and, when faced with a dilemma, choose that alternative which creates the greatest good for the greatest number of people."

3. **Divine commandments.** A belief in God and a desire to do as God has commanded has historically been the most important criterion for deciding right and wrong. If God says, "Thou shalt not..." those who believe accept it as wrong. For these people, the ultimate test of whether something is right is based in the word of God.

   One principle, then is "never do that which is condemned by God."

4. **Natural laws.** Right and wrong must be consistent with natural laws and human nature. Actions that are good are in harmony with principles that contribute to personal growth, a peaceful society, and the development of character. If something violates a natural law or is inconsistent with human nature, it is considered wrong.

   For example, lying and stealing are immoral because they damage the inherent relationships between people and destroy personal character.

   The principle is "never behave in ways that are inconsistent with natural laws or the duties and obligations placed on you by human nature."

5. **Reason and logic.** A crucial test of whether something is moral is based on a universal standard of justice and fundamental fairness. Is it just, fair, and right to everyone, recognizing the unique differences of individuals that may require differential treatment? Is it consistent with clear reason and sound logic? Can it be universalized, and does it respect the agency and dignity of individuals?

   The principle here is "never take any action that you would not be willing to see others, faced with the same situation, also be free to take." This principle is also called "universalism."

The King II report urges organisations (both private and public) to adopt ethical codes which, if supported by effective communication channels & training, and is seen to be enforced, could contribute to the development of a moral business culture in South Africa.

A suggested Ethical Decision Making Model for all Employees:

1. Evaluate information
2. Consider how your decision might affect stakeholders*
3. Consider what ethical values** are relevant to the situation
4. Determine the best course of action that takes into account relevant values & stakeholders' interests

* Employees, clients, suppliers, shareholders, communities

** Honesty, integrity, respect, trust, responsibility, citizenship

COMPILING A FRAUD PREVENTION AND DETECTION PLAN

Preventive controls are applied before the event and are intended to restrict access, pin down accountability for certain actions and provide a deterrent against fraud. **Detective** controls are applied at or after the event. Not all risks can be prevented and so reactive controls monitor performance and report on deviations.

The plan needs to cover the following areas:

- Objectives – the goals to be achieved, principles of ownership, the nature of specific controls and the need for continuing evaluation of risks.
- Scope – to which areas of the company the plan applies to.
- Responsibilities – of operational managers, internal audit, the audit committee and security.
- Compliance Declaration – employees are to provide annual letters stating that they have complied with the plan, that they have reported all fraud-related incidents and are not aware of any areas of weakness.
- Cost Justification – how success will be evaluated.
- Incident Reporting – procedures for reporting fraud.

There are a number of principles that must be addressed in the policy:

- Security will be assured through controls, which function as specified.
- Each function must have a designated owner.
- Owners must be held accountable for the process under their control.
- Owners must have the authority to discharge their responsibilities.
- Owners must be held accountable for failure/short cuts.
- Since most owners will not have general or specific fraud awareness, they must be given guidance on risks and instruction on the controls to be maintained – an intensive one-day fraud awareness workshop with annual reinforcement training is recommended.
- Line management/supervisors are responsible for ensuring that controls function as specified.
- Standards must be issued to owners on a ‘need to know’ basis – people planning fraud should not be able to assess controls outside their areas of responsibility.

The Audit Office of New South Wales, Australia, recommends the following ‘Ten Best Practice Attributes of an effective Fraud Control strategy’:

1. Integrated Macro Policy – establish a holistic & functionally integrated fraud control strategy.
2. Responsibility Structures – assign strategy implementation & co-ordination responsibility.
3. Fraud Risk – measures to be taken to ID fraud risk areas & develop countermeasures.
4. Employee Awareness – plan of action to raise fraud awareness & modify fraud attitudes.
5. Customer Awareness – action plan to raise level of client awareness regarding fraud prevention.
6. Fraud Reporting Systems – implementation of effective internal fraud reporting systems.
7. Protected Disclosures – implementation of policies to protect whistle-blowers.
8. External Notification – policy implementation for reporting suspected/known fraud to authorities.
9. Investigation Standards – develop mechanisms for investigating frauds from beginning to end.
10. Conduct & Disciplinary Standards – establish policies, standards, systems and procedures relating to conduct and discipline which support the fraud control strategy.

K. CONDUCTING FRAUD AWARENESS PROGRAMS

In our opinion, everyone, from the Managing Director of a 'Top 200' Corporation to the sole proprietor, should know how to fight fraud, as only the well informed can deter it.

Regular Fraud Awareness Training for relevant staff will protect your organisation by:

- creating an awareness about fraud
- familiarizing staff with actual fraud cases
- reducing incidences of fraud
- helping to deal with actual fraud cases in progress
- explaining how to recover some, if not all, monies lost to a fraud
- preventing the same or similar frauds from recurring
- emphasizing the importance of preventative measures
- presenting the pros & cons of using computers for financial transactions

We believe that a lack of awareness/education seems to be one of the biggest problems in most South African organisations. In order to combat fraud it is essential that we understand who the enemy is, how they accomplish what they do, and know what options are available to protect ourselves. The 'big 4' accounting firms all say the same thing about fraud, and that is 'they obtain approximately 90% of their fees from Fraud Investigations and only 10% from Fraud Prevention'. This situation must be reversed if we are to beat fraud.

In the two Ernst & Young and KPMG Fraud Surveys 66% of the respondents admitted to having experienced fraud recently. 88% of respondents **perceived that fraud would increase – yet 60% of respondents said that their staff had not received fraud awareness training** and also had not conducted a review of their business's vulnerability to fraud! Many companies are turning to EFT (Electronic Funds Transactions) to try and prevent cheque fraud, yet in these surveys only 10% of respondents were confident that corporate controls were in place to prevent computer hacking!

Many corporations and banks can testify to the fact that cheque fraud in their organisation has been dramatically reduced and one of the main reasons has been education of their staff. As you will see, 'Reinforcement' is critical to training, and if the same message is hammered home regularly as opposed to just once, the individual retains at least 50% more of what he/she has seen & heard, and the sponsoring company gets value for money.

Both Company A and Company B spend R100 000-00 annually training their employees. Both companies have defined goals and feel that training is an investment to help achieve those goals. **Company A** spends all of its money on training assuming that "If I train… they retain," and subsequently implement. **Company B** understands the value and necessity of Periodic Reinforcement. It allocated 10% of its training budget to Reinforcement. Furthermore, it contracted a specialist company who had an impressive track record to develop and implement a cohesive Reinforcement Program.

The net result is that **Company B** has finished way ahead. **Company A** needs to spend R1.1 million more on training to accomplish what Company B did with R10 000-00 on Reinforcement.

Flowing from the public seminars (like the CPE13), various in-house training sessions have been held, the aim of which is to create awareness at coalface level within the organisation regarding

fraud. This is often where a fraud can be turned into an "attempted" fraud. Such awareness substantially enhances an organisation's chances of reaping rewards from their risk management strategy.

"Corporate fraud prevention training in most organisations is negligible," the Institute of Chartered Accountants' Fraud Advisory panel (FAP) warned in their 1998/99 annual report.

"The two main problems in the fraud prevention battle are: lack of awareness and lack of training. Despite almost daily reminders in the press that no section of society is immune from the risk of fraud, prevention is not seen as the responsibility of anyone in particular within most organisations. The burden is shared haphazardly between various departments. Training, therefore, tends to be equally haphazard."

George Staple, FAP's chairman said, ***"The resources for those who are the 'guardians' against fraud within companies are slight. You can trace this back through the educational institutions themselves. You would expect them to provide – as part of professional courses – training in detection and prevention of fraud, but very few have anything in place."***

"Until it happens, you don't realise what the trauma is, the loss that can be suffered and the impact on people's lives. Until the company suffers, senior management never focuses on the subject of fraud. They think it always happens to someone else."

In the 1998 Association of Certified Fraud Examiners worldwide member survey, two very important questions were asked:

- Does management allow adequate resources to prevent and detect fraud? **75% answered *NO***.
- Is management co-operative during fraud investigations? **82% answered *YES***.

It would seem that management is not prepared to spend a little time and money on preventing fraud, but once the fraud has occurred then all the time and money that is needed is freely given (penny-wise, pound-foolish?). Closing the barn door once the horse has bolted is a common corporate trait.

The problem of fraud is essentially financial, but there seems to be no history of systematic training in fraud prevention within the accountancy profession, with the exception of the Institute of Internal Auditors. There also does not appear to be any graduate training in fraud prevention for managers. A poll of MBA providers & students could find no evidence of any formal fraud training.

This appears to reflect the fact that anti-fraud measures are not seen as a serious commercial necessity. Anti-fraud training programs should, therefore, become a priority in organisations and should reflect the fact that staff at all levels should take appropriate responsibility for fraud. Training needs to be relevant, practical and effective. (A number of delegates at previous training courses commented that while their organisations give fraud prevention and detection a high priority on paper, this often does not translate into practical strategies such as education of staff).

LEARN FROM OTHER'S MISTAKES – LESSONS FROM LEESON

A reputable and seemingly rock-solid player in the London financial world was Barings Merchant Bank. This was a respected, professionally led bank with a lineage of over 200 years. The bank attracted the accounts of the blue-blooded & of the royal family. Barings had also moved into derivatives & had taken on a number of people who had not traveled the orthodox upper-class path.

One of these new boys was Nicholas Leeson. He worked in the back office where deals are cleared administratively but which is also the first line of defense against fraud. Because he failed to disclose a few court debt injunctions on his application to join the London stock market he was banned from working on that exchange – Barings sent him instead to Singapore. He was 25 years old and his rise was meteoric. In 1993 he made handsome profits for Barings, but on 17 January 1995 Leeson's world began to unravel when Japan was hit with a large earthquake causing the Nikkei to dip.

Instead of pulling out the market, with his damages severe but limited, Leeson tried to fight the market. The Nikkei slumped further and a few days before his 28th birthday, Leeson left a note on his desk saying 'sorry' & was later arrested in Germany until he was extradited to Singapore.

How could one man escape the controls & cause the 6th largest merchant bank in Britain to crash out of the blue? As with many cases of corporate deviance there were many 'red flags':

- "I knew from my experience… that when it came down to detail, ***no managers actually wanted to get their hands dirty & investigate the numbers.*** They always felt they were above that…"
- As early as March 1992 Barings management knew that Nicholas Leeson was dishonest when it was found that he had twice lied about judgments issued against him for debt. Barings had fidelity insurance of $100 000 000.00, but coverage is invalidated "when any person not in collusion with the miscreant has knowledge of his dishonesty and fails to report it".
- He was granted a great deal of autonomy and operated not only in the dealing room but also in the back office, whereas these two functions should be separated in order to enhance control.
- Leeson's manager, Mary Walz, always accepted non-answers to her thorough instructions.
- He made use of office politics and matrix (decentralised) management, to avoid accountability.
- Tony Railton, ***the internal auditor, accepted 'Gobbledygook' answers***.
- In 1995 Leeson forged a letter of indebtedness for $78 million to cover his $50M trading losses. Coopers & Lybrand agreed the figures even though the forged letter was blatantly obvious.

These important lessons are related to banking, business and management. Organisations seek predictability and solid rewards, but change and fierce competitiveness produces volatility and risk-taking - and reputation, integrity, and controls can all be undermined by a management that refuses to change, refuses to face up to reality, becomes blinded by success, becomes seduced into short-term decision-making, ignores warning signs, and that indulges in scapegoating and conspiracy theories when confronted with the consequences of its own incompetence. **The Barings directors simply did not understand their own business.**

It's difficult to legislate for greed and stupidity – but greed and stupidity are social and cultural constructs that are enhanced by specific times and particular settings. The Barings incident is of value in informing us about the fragility of financial markets, about the vulnerability of control systems, and about the weaknesses that can afflict management. Of course, if Leeson had been right in his judgment, he would now be a rich hero instead of an ex-convict.

L. FRAUD DETECTION

With the best will in the world management cannot totally eliminate fraud. In this eventuality organizations must be equipped with the methods of detecting fraud. So how can management detect fraud in an organization? Usually fraud detection is not discovered by deliberate methods but rather by the checks & balances or accidents. The following are excerpts relating to fraud detection from "Fraud Auditing and Forensic Accounting - G. Jack Bologna and Robert J. Lindquist":

"Detecting fraud is a matter of acknowledging:

- That fraud exists;
- That any organization can become either a victim of fraud or a perpetrator of fraud
- That certain weaknesses in *internal controls &* human character can be conducive to fraud.
- That certain tests of internal controls and tests of the organization's motivational environment can provide some insight on the possibility of fraud in that environment.
- That the key to fraud auditing is training the mind to see both the doughnut and the hole."

"…a few exceptions fraud auditors should look for: Transactions that are odd as to:

- Time (of day, week, month, year, or season)
- Frequency (too many, too few)
- Places (too far, too near, and too far out")
- Amount (too high, too low, too consistent, too alike, too different)
- Parties or personalities (related parties, oddball personalities, strange and estranged relationships between parties, management performing clerical functions)
- Internal controls that are unenforced or too often compromised by higher authorities
- Employee motivation, morale, and job satisfaction levels that are chronically low
- A corporate culture and reward system that supports unethical behavior toward employees, customers, competitors, lenders, and shareholders"

"RED FLAGS" OF MANAGEMENT AND CORPORATE FRAUD

In every case of management and corporate fraud, telltale signs of the fraud existed for some period of time before a third party detects or discloses it. These signs may be:

- Significant observed changes from the defrauder's past behavior pattern.
- Knowledge that the defrauder was undergoing emotional trauma in his home life or work life.
- Knowledge that the defrauder was betting heavily, drinking heavily, had a very expensive social life, or was sexually promiscuous.
- Knowledge that the defrauder was heavily in debt.
- Audit findings deemed to be errors & irregularities that were considered immaterial at the time.
- Knowledge that the company was having financial difficulties such as frequent cash-flow shortages, declining sales and/or net profits, and loss of market share,
- Knowledge that management was showing increasing signs of incompetence; i.e., poor planning, organization, communication, controls, motivation, and delegation; management indecision and confusion about corporate mission, goals, and strategies; and management ignorance or conditions in the industry and in the general economy.
- Substantial growth beyond the industry norm in regulated industries."

"**BADGES" OF TOP-MANAGEMENT FRAUD:**

- Tend to have highly material personal values. Success to them means financial success, not professional recognition.
- Tend to treat people as objects, not individuals, and often as objects for exploitation.
- Are highly self-centered.
- Are often eccentric in the way they display their wealth or spend their money. They tend to be conspicuous consumers and often boast of the things they have acquired, the friends they have in high office, and all the fine places they have visited.
- Speak about their cunning achievements and winnings more than their losses.
- Appear to be reckless or careless with facts and often enlarge on them,
- Appear to be hard working, almost compulsive, but most of their time at work is spent in scheming and designing short cuts to get ahead or beat the competition.
- May gamble or drink a great deal.
- Buy expensive gifts for their families, usually to compensate for spending little time with them.
- Are hostile to people who oppose their views. They feel exempt from accountability and controls because of their station or position.
- Create a great deal of turnover among their subordinates and often set off one subordinate against another
- Play favorites among their subordinates, but the relationship can cool very quickly because a subordinate often falls from grace after one mistake, even an insignificant one.
- Manage by crisis more often than by objectives. They tend to drift with the times and have no long-range plans.
- Tend to override internal controls with impunity & argue forcefully for less formality in controls.
- Demand absolute loyalty from subordinates, but they themselves are loyal only to their own self-interests.
- Have few real friends within their own industry or company. Their competitors and colleagues often dislike them."

"**RED FLAGS" OF LOWER-LEVEL FRAUD:**

- Their superiors exert great pressure to achieve high performance-higher sales, lower costs, and more profits. Top management tolerates no justification or excuse for less than expected or demanded sales, cost, and profit targets.
- Bonuses are tied to short-term performance levels and do not take into consideration economic or competitive realities.
- Internal controls are absent or loosely enforced.
- Management controls consist mainly of pressures for performance: "Make your numbers come out right or we'll get somebody else."
- Business ethics are subordinated to economic self-interest.
- Vendors and suppliers are squeezed for the last ounce of profitability in their goods and services.
- There is a great deal of confusion about duties and responsibilities among subordinates.
- A high level of hostility exists among subordinates and between lower-level managers and their line and staff superiors.
- They believe the present level of responsibility exceeds the original job description."

Using CAATTS to detect fraud

Talking to other auditors about their use of Computer Assisted Audit Tools and Techniques (CAATTs) can be enjoyable and informational. However, when asked to explain their use of CAATTs auditors often reply that the tools offer the ability to 'dump data to a spreadsheet, sort it and then print it out.' Certainly, getting the required data and reading it electronically are important steps, but why simply sort it and print it out?

Today's auditors must possess more than a passing acquaintance with the strength and utility of audit software like ACL. The ability to truly use data allows auditors not only conduct routine audits, but also "value for money audits". There are other audit tools that can be invaluable in detecting fraudulent activity but we will be discussing the ACL product.

Fraud Detection with ACL

ACL has become a mission-critical software tool for detecting and preventing fraud for auditors around the world.

How extensive is fraud? What is it costing your organization? How do you detect and discourage fraud? These are some of the questions facing audit departments today. Even the simplest of frauds is difficult to detect when faced with millions of transactions. The data analysis capabilities of ACL offer a host of new opportunities to detect and deter fraud while supporting the requirement to review large volumes of transactions. ACL includes the ability to:

- compare employee and vendor addresses to identify employees who are also posing as vendors
- identify vendors using PO Box addresses
- identify missing or fraudulent checks or invoices by analyzing the sequence of all transactions
- identify all vendors with more than one vendor code or more than one mailing address, or multiple vendors sharing the same mailing address
- sort payments by amount to identify transactions that fall just below financial control or contract limits

ACL offers a wide range of commands and functions specifically designed to assist in analyzing and understanding data when identifying and quantifying fraud. As a result, ACL has become a mission-critical software tool for detecting and preventing fraud for auditors around the world.
Some of the most useful techniques include:

Gaps
The ‘Gaps’ command checks the data for breaks in a series or sequence. The entire file can be examined to see if all items are accounted for and properly recorded. In reviewing health claims, for example, finding claim numbers that are out of sequence or missing can help focus the search for fraudulent claims. If claims are submitted on pre-numbered forms, testing to see if the claim numbers correspond to the expected numbering sequence is one way to isolate potentially fraudulent claims.

Duplicates
In many cases, fields should contain only unique values, such as invoice numbers. The Duplicates command checks the file for duplicate values in key fields. For example, you can search for duplicate invoice numbers or duplicate travel claims for the same time period.

Classify
The Classify command counts the number of records relating to each unique value of a character field and accumulates totals of specified numeric fields for each of those values. Your results can be output to the screen, a text file, or a data file. With a single command, you can determine the total revenue and expenditures, by account and for every branch, in the company.
This provides a basis for comparative analysis and a quick method of identifying incorrect data, such as invalid accounts, in which fraudulent transactions may be hidden.

Trend Analysis
Trend analysis allows you to compare information from several periods or locations, and helps to identify anomalies in the operations of a business unit. Audits conducted in the same operational area on a regular schedule are ideal candidates for trend analysis. The current period's data can be combined with previous periods and trends used to examine and highlight areas for further attention. Comparisons of business operations in different locations, for example, can quickly identify areas of concern. Comparison of the rate of return due to defects, by vendor, may indicate acceptance of inferior goods in return for a kickback from the vendor.

Join
The Join command combines information from two or more data files into a single file, and can pinpoint unusual transactions. Although the information may be stored in different files or databases, ACL allows you to physically join the files, or logically relate the information from many files, creating a single file with related information from the files used to create the Join. There are five possible ways to Join files, however, space limitations prevent detailed discussion of them here. Join can highlight records that should match, but do not. For example, all employees should have some deductions. Joining the personnel file and the payroll file can identify all employees with no payroll deductions. Alternatively, all payroll transactions recorded against "employees" not in the personnel file would show up.

Relations
Relations works much like Join, allowing you to simultaneously access data from up to 18 files. By doing so, expected relationships can be confirmed and unexpected relationships highlighted. For example, you would expect a relationship to exist between every name in the master employee file and the payroll transaction file. However, you would not expect a relation to exist between the master employee file and the master vendor list. Relations would also confirm the existence, or absence, of a purchase order number for every invoice, or that purchases by a particular employee are below the authorised limit.

The use of ACL to analyze electronic data, to identify anomalies, trends and duplicates can be invaluable when performing audits. The use of audit software can also be extremely useful in detecting fraud. Matching data, joining files, recalculating amounts and totals are performed easily and can identify serious exposures. When fraud is detected, the use of tools like ACL can also help the auditor to quantify the amount or extent of the losses.

ACL Services Ltd. can be found at **www.acl.com** or **www.cqs.co.za**

Benford's Law

More advanced techniques take data analysis to another level, examining the actual frequency of the digits in the data. Benford's Law, developed in 1938 by Frank Benford, a General Electric physicist, makes predictions on the occurrence of digits in the data. Benford's Law concludes that the first digit in a large number of transactions will be a '1' more often than a '2', and a '2' more often than a '3' and so on. Benford calculates that the first digit will be a '1' about 30% of the time, whereas '9' only has an expected frequency of about 5% as the first digit.

Benford's Law applies to any data set:

- Which is not based on assigned numbers, such as policy numbers or tax reference numbers
- Where there is no arbitrarily assigned maximum or minimum value in the set, such as a file of purchase orders applying to an employee with a limited authorisation level
- Where there are no price break points, such as R6.50 for all packages under 1 kilogram

Probability of Detection

The biggest problem with the above techniques is that people are reluctant to try them, usually because they don't believe that they could be lucky enough to detect the Nick Leeson in their organisation. In fact the probability of success in detecting fraud is very high and depends on the size of the organisation, the number of items tested, and the number of fraudulent items in the data.

As an example, if there are 8 white balls and 2 black balls in a bucket, and tests are made to detect the presence of black balls by drawing three random balls, the probability of drawing at least 1 black ball is greater than the pure percentage chance of 25%. There are 120 possible combinations of 3 balls and 56 possible combinations of only white balls. The failure rate is therefore 56 over 120 (47%) and the success rate is 53% by making a test on just 30% of the data.

FRAUD HOTLINES

It is unlikely that fraudsters will be able to conceal their every move, and employees need to be positively encouraged to report any incident or circumstance that they think may compromise the organisation's security. There must also be clear channels for employees to go through and guarantees that nothing will be held against them even if their suspicions are mistaken.

Fraud should be a regular topic for discussion at staff meetings as opposed to the existing attitude in many companies where managers don't want to deal with fraud because they don't want to admit fraud exists. It has been said that companies often do not discuss fraud for fear of adverse publicity. To quote Business Against Crime – Kwa-Zulu Natal, ***"In contemporary South Africa it is more likely that the opposite is true, for such is the scale of commercial crime that there are no organisations which are not affected, & an organisation with a clean crime record is itself liable to speculation that it is soft on crime and therefore not protective of shareholders interests".***

Anonymous toll-free hot-lines seem to be very effective in encouraging both insiders and outsiders to report their suspicions of fraud – even low-level fraudulent activities that may lead to much bigger frauds.

We would recommend the implementation of a reward program for the successful prosecution and recovery of defrauded monies and, most importantly, to give staff feedback on each case. We have found that anonymous toll-free hot lines and reward programs get very good results:

- The Auditor General in Kwa-Zulu Natal installed a toll-free hot-line in January 1997 and by January 1998 they had received over 5000 calls, the majority of which were false alarms or hoaxes, but they did get approximately 450 prosecutions.

- Nedbank started a 'Beat the Bandits' campaign in June 1997, which included a toll-free hot-line and a reward program, and since then fraud losses have been reduced by 37% and over 1100 rewards have been paid out to staff, totaling more than R1.5 Million.

- FirstRand introduced a staff incentive scheme in April 1999 as part of a crackdown on white-collar crime. Staff who prevent potential fraud would qualify for a monthly draw for R25 000.00. At the end of the year all qualifying entrants would be entered into a draw for the grand prize of R1 Million. Standard Bank has since done a similar thing.

Despite the fact that fraud prevention should form part of the employee's job description anyway, the receipt of a bottle of wine or a special lunch can have a considerable effect on morale and motivation. When rewards are being offered, however, each case of prevented or detected fraud must be investigated to ensure that the staff member did not perpetrate the fraud in order to 'detect' it and so receive the reward.

The King II report urges organisations (both private and public) to facilitate confidential whistle-blowing mechanisms and to ensure that justified whistle blowers are not penalised, but praised for their efforts on behalf of the organisation.

The Public Finance Management Act, No 1 of 1999, places a responsibility on the Accounting Officer to, among others, take effective and appropriate steps to prevent unauthorised, irregular and fruitless and wasteful expenditures and losses from criminal conduct. The Sarbanes-Oxley Act of 2002 has a whistle-blowing mechanism as a legal requirement for any public trading company. The Protected Disclosures Act, No 26 of 2000 recognises that:

- Every employer and employee has a responsibility to disclose criminal and other irregular conduct in the workplace and
- Every employer has a responsibility to take all necessary steps to ensure that employees who disclose such information are protected from any reprisals as a result of such disclosure.

Internal or External Mechanism

Some organisations provide an internal hotline as an option for employees who are uncomfortable discussing issues face-to-face. Calls to the hotline are frequently routed to an employee somewhere in the organisation, usually in Human Resources or Internal Audit. This solution may seem attractive from an expense point of view but there are some serious drawbacks:

- If employees know they are phoning or e-mailing an internal source they may be afraid that they will be identified by voice recognition or e-mail address respectively;
- There may be inconsistent handling of sensitive calls;

- Callers may encounter a voicemail; and
- An internal hotline leaves the organisation vulnerable to allegations of covering up issues involving management.

An external facility provides greater safeguards of anonymity and avoids even the appearance of impropriety. While there are costs associated with an external hotline the financial investment is small in comparison to the potentially disastrous results of unethical activity that goes undiscovered.

We have, however been told by many organisations that their hotline doesn't work. Some organisations then resort to paying rewards. Rewards may work but they may also backfire. Keep in mind that the Protected Disclosures Act stresses that the whistleblower will not be protected if they are paid a reward. Also, we have found that employees could perpetrate the fraud in order to get their name/s in the monthly lucky draw! This means that every alleged fraud must be investigated thoroughly to see that this is not happening.

The Rollout is the most critical phase of the hotline process yet many organisations take short cuts here. This is definitely being 'penny-wise pound-foolish' as a rollout that is done to all staff members annually will determine whether the hotline is a success or failure. Just putting up posters and keeping your fingers crossed will not ensure that employees know the why, what, when, and how of your whistleblowing mechanism.

We are often called into organisations to evaluate their existing hotline and we then survey a sampling of staff and we normally get the following feedback:

- We have a Hotline!?
- It's only a suspicion – I don't have evidence
- It's not my problem
- I don't want to be a sneak
- Nothing will be done
- It'll only cause trouble
- How far up does it go?
- What if I'm wrong?
- What if my voice is recognized?

These concerns are all valid and exist because employees were not adequately educated via the rollout process, or the rollout was a once-off with little or no reinforcement. In our opinion, the rollout should be done every 12 – 18 months and it needs to be done for all staff, not just a select few.

When installed properly an independent and anonymous whistle-blowing mechanism can unearth a variety of items that can improve processes, resolve issues and prevent huge financial losses. A fraud hotline was once just a luxury that large organisations implemented. Now it is a competitive business advantage for enlightened organisations of all sizes.

PROACTIVE FRAUD AUDITING: A FIVE-STEP APPROACH

…as recommended by the Institute of Internal Auditors:

1. IDENTIFY THE EXPOSURES
2. KNOW THE SYMPTOMS OF OCCURRENCE
3. BE ALERT FOR SYMPTOMS
4. BUILD AUDIT PROGRAMS TO LOOK FOR SYMPTOMS
5. FOLLOW THROUGH ON ALL SYMPTOMS OBSERVED

1. Identify / Know the exposures - Know what can go wrong and who could do it. Know what opportunities there are for employees, managers, outsiders, suppliers, agents and others providing goods and services. For cooking the books, know the pressures for favourable results. Understand the systems and controls, and what they are intended to prevent or detect. An annual Fraud Health Check-Up will provide the exposures.

2. Know the symptoms of occurrence - Symptoms are specific. Symptoms may be of the fraud itself, or of the cover-up attempt. For each exposure, know how it would be reflected in documents, reports, paid cheques, reconciliations, accounts, complaint files, and adjusting or correction entries.

Symptoms of fraud can be divided up into six different categories. These categories are:

- *Accounting anomalies* - When searching for fraud, it is helpful to look for sudden changes in account balances. Significant differences in accounts may arise from faulty journal entries and inaccuracies in ledgers.
- *Internal control weaknesses* – An analysis should be performed to identify areas that have weak or no controls present. This is important because weak controls can be easily overridden when pressure arises to commit fraud.
- *Analytical anomalies* – An analysis of transactions can reveal amounts that are too large or too small for accounts. These accounts should be examined for fraud.
- *Extravagant lifestyles* – Managers should take time to analyze the lifestyles of their employees. Unexpected and unexplained changes in lifestyle may suggest that fraud has taken place. The activities and responsibilities of these employees should be monitored.
- *Unusual behaviours* – Managers should take time to notice emotional changes of employees. Stress and fear are good indicators that an employee may be committing fraud.
- *Tips and complaints* – Managers should review complaints and tips made by employees. Complaints and tips may provide clues to who is committing fraud.

3. Be alert for symptoms - Many cases are detected by an auditor or operations manager following through on a symptom noted while actually looking for something else.

4. Build audit programs to look for symptoms - Determining exposures and evaluating internal control precedes writing the audit program. Some environments may lack controls, which the auditor can rely upon to protect the organisation's interests. Such environments include some remote locations and outsiders such as vendors, agents and contractors. Even in organisations with good controls, frequently there are areas or departments lacking segregation of duties or meaningful supervisory review.

In developing the audit program the auditor should include specific steps designed to look for symptoms of fraud. Sampling plans should take into consideration the fraud stratification of the population; stratified sampling, directed sampling, and discovery sampling may prove to be helpful. In the completely uncontrolled environment the auditor will want to determine the tolerable undetected fraud allowable in the population. The auditor may want to design his sample so as to include a fraudulent occurrence should the level of fraud in the population aggregate more than the tolerable amount.

Note: No fraud is acceptable. But auditors in deciding sample sizes actually are determining the probability of having the opportunity to detect fraud. The probability is dependent upon the amount of fraud, the size of the population and the sample selected.

5. Follow-through on all symptoms observed - The auditor should resolve all symptoms. The auditor should operate with an attitude of healthy professional skepticism. Beware of pressures to complete work on time. Be aware that the single symptom you are looking at may not be an isolated occurrence; it may be one of many.

FRAUD PREVENTION is by far the most cost-effective approach.

FRAUD DETECTION, and prosecution of all offenders, are the best prevention tools.

Fraud is everyone's problem …
As it affects bonuses, salaries, pensions and even jobs.

FRAUD INVESTIGATION

The responsibility for the prevention and detection of fraud rests with the organisation's management (and with the internal & external auditors in the case of financial statement fraud). Once the evidence of fraud is presented the fraud examiner/forensic auditor is expected to perform sufficient procedures to resolve the fraud allegations. Fraud examination is a methodology for resolving fraud allegations from inception to disposition. Fraud examination incorporates many auditing techniques and many fraud examiners have an accounting background and although they seem related they are not the same discipline. The following table lists some of the main differences:

Auditing vs. Fraud Examination		
Issue	**Auditing**	**Fraud Examination**
Timing	***Recurring***	***Non-Recurring***
	Audits are conducted on a regular, recurring basis	Fraud examinations are non-recurring. They are conducted only with sufficient predication.
Scope	***General***	***Specific***
	The scope of the audit is a general examination of financial data.	The fraud examination is conducted to resolve specific allegations.
Objective	***Opinion***	***Affix Blame***
	An audit is generally conducted for the purpose of expressing an opinion on the financial statements or related information.	The fraud examination's goal is to determine whether fraud has occurred, is occurring or will occur, and to determine who is responsible.
Relationship	***Non-Adversarial***	***Adversarial***
	The external audit process is non-adversarial in nature.	Fraud examinations, because they involve efforts to affix blame, are adversarial in nature.
Methodology	***Audit Techniques***	***Fraud Examination Techniques***
	Audits are conducted primarily by examining financial data.	Fraud examinations are conducted by (1) document examination; (2) review of outside data such as public records; and (3) interviews.
Presumption	Professional Scepticism	***Proof***
	Auditors are required to approach audits with professional scepticism.	Fraud examiners approach the resolution of a fraud by attempting to establish sufficient proof to support or refute an allegation of fraud.

The forensic auditor is not normally responsible for the initial detection of fraud and only becomes involved after an allegation of fraud has been made. The forensic auditor responsibilities are to: obtain evidence, take statements, write reports of fraud examinations, testify to findings, and assist in the detection and prevention of fraud.

Each fraud examination begins with the proposition that all cases will end in litigation. Fraud theory begins with the assumption, based on the known facts, of what might have occurred. That assumption is then tested to determine whether it is provable. The fraud theory approach involves analyzing available data, crating a hypothesis, testing the hypothesis, refining and amending the hypothesis, and then accepting or rejecting the hypothesis based on the evidence.

THE FRAUD RESPONSE PLAN

The Fraud Response Plan (FRP) is a step-by-step process of the procedures that should be followed by management, should an incident of fraud occur. Too often, an organisation experiences an incident of fraud but management are not aware of what to do, exposing the organisation to cases where recoverability becomes nearly impossible and/or the exposure of IR disputes becomes apparent.

The King II report urges organisations (both private and public) to prepare disaster recovery plans to ensure continuity of their operations in the event of a catastrophe.

ACTION	COMPLETED BY	DATE COMPLETED
Secure documents and relevant evidence relating to the suspected fraud;		
Secure the contents of the suspect's office or workstation, personal computer, diary and files, including all personal documents on the premises;		
Locate and secure any of the above, should they have been removed by the suspect;		
Counter the undermining of staff morale or interference in the investigation by removing the suspect from the premises – cancel parking/access cards; withdraw signatory authority and change passwords or access codes;		
Inform the HR Department in writing;		
Inform the representative responsible for tracking all incidents of fraud;		
Commence an investigation, with the initial aim of establishing the scale of the offence and the degree of contamination within the company and to all business partners, and to effect improved internal controls;		
Do a preliminary assessment of the following issues: • Disciplinary hearing (HR); • Civil & criminal proceedings; • Insurance claim (Insurance Broker).		

NOTE: *The FRP should be endorsed by the CEO or MD and circulated to all members of management. It must be stressed that the FRP must become a working company policy. In addition to an effective FRP, an organisation will need Expert legal assistance, and Expert investigative assistance. A victim, looking to recover losses, does not want to be led up a blind alley of drawn-out and costly legal action. It is therefore important to choose advisors who have the skills to pursue the fraudsters, across borders if necessary, and also the ability to recover the assets. An investigation is pointless if assets cannot be recovered, proceedings cannot be instituted against the suspect, or long and expensive labour litigation results from incorrect actions from management.*

M. APPLICABLE LEGISLATION

There are various laws that deal with issues governing fraud and corruption, but there are primary laws that you need to be aware of in the operations of a business, irrespective of its size.

"..And whereas corruption and related corrupt activities undermine the rights (in the Bill of Rights), endanger the stability and security of societies, undermine the institutions and values of democracy and ethical values and morality, jeopardise sustainable development, the rule of law and the credibility of governments, and provide a breeding ground for organised crime; … ".

In terms of its principle of legality, the criminal law must first be satisfied that the conduct in question falls within the common law or statutory definition of an offence. The first law that any person should be familiar with is criminal law which covers fraud and related offences like bribery, forgery and embezzlement. Thereafter, other legislation (as disclosed below) needs to be understood so that one's responsibility thereto is not overlooked.

Other legislation:

Prevention of Organised Crime Act 121 of 1998 (POCA)

This is a powerful statute. It creates a number of offences relating to racketeering. One of the offences listed that can constitute a "pattern of racketeering activity" is corruption as contained in the new Act. Once there are proceeds generated by corruption, whether related to racketeering or not, such proceeds – or property into which it is converted – are liable to confiscation if a conviction ensues or to forfeiture notwithstanding no prosecution was instituted.

Money Laundering

The Proceeds of Crime Act 76 of 1996 was repealed and its *money-laundering* provisions incorporated into the Prevention of Organised Crime Act ("POCA") of which sections 4, 5, 6 and 7 contained money-laundering offences. These provisions are relevant to our subject in that a member or employee who uses his/her position in an institution to assist a money-launderer is liable to severe penalties.

Section 4 specifically states that

- Any person who knows, or ***ought reasonably to have known***, that property is or forms part of proceeds of unlawful activities, and
- Enters into agreement, arrangement or transaction with anyone in connection with that property, whether legally enforceable or not or
- Performs any other act with such property which has or is likely to have the effect -
  - Of concealing or disguising the nature source, location, disposition of property or ownership thereof or
  - Enabling or assisting any person who has committed an offence,
  - To avoid prosecution
  - To remove or diminish any property acquired as a result of unlawful activity

Commits an offence

Section 5 specifically refers to knowingly assisting another in a money laundering transaction.

Section 6 specifically refers to knowingly acquiring, using or possessing property that is the proceeds of unlawful activity.

Section 7 specifically refers to failure to report any transaction suspected of involving money laundering

Section 4, 5 and 6 carries with it a fine not exceeding R100 million, or to imprisonment for a period not exceeding 30 years, while Section 7 carries a fine or imprisonment not exceeding 15yrs

Protected Disclosures Act (PDA)

The Act provides for employees, in both public and private sectors, to disclose information regarding the unlawful or irregular conduct ("impropriety") of an employer, or an employee of that employer without fear of being subjected to "occupational detriment". The relevance to our subject is that as corruption is hard to detect or prove that the whistleblower or the act of whistleblowing is protected. Three key requirements are viewed, namely (1) disclosure must be made in good faith, (2) the disclosure must be done via approved company procedures/policies and (3) the disclosure must not have been made for financial gain/reward.

Prevention and Combating of Corrupt Activities Act 12 of 2004 (PRECCA)

PRECCA is a comprehensive act and covers general as well as specific offences. Key word utilized throughout this act is "gratification" which is very widely defined to indicate that any benefit is included.

Gratification as defined by the act includes the following:

- *Money whether in cash or otherwise;*
- *Any donation, gift, loan, fee, reward, valuable security, property or interest in property of any description, whether movable or immovable, or any other similar advantage;*
- *The avoidance of a loss, liability, penalty, forfeiture, punishment or other disadvantage;*
- *Any office, status, honour, employment, contract of employment or services, any agreement to give employment or render services in any capacity and residential or holiday accommodation;*
- *Any payment, release, discharge or liquidation of a loan, obligation or other liability, whether in whole or in part;*
- *Any forbearance to demand any money, or money's worth or valuable thing;*
- *Any other service or favour or advantage of any description, including protection from any penalty or disability incurred or apprehended or from any action or proceedings of a disciplinary, civil or criminal nature, whether or not already instituted, and includes the exercise of forbearance from the exercise of any right or any official power or duty;*
- *Any right or privilege;*
- *Any real or pretended aid, vote, consent, influence or abstention from voting;*
- *Any valuable consideration or benefit of any kind, including any discount, commission rebate, bonus, deduction or percentage".*

In the act reference is made to state that (a) any person (b) who accepts (etc) or who gives (etc) (c) any gratification (d) to any other person (e) in order to act (f) in a manner (g) that amounts to a result or an effect

Although there are many definitions of corruption (as disclosed in previous section covered), the general offence of ***corruption as defined by PRECCA*** is as follows:

- *"Any person, who, directly or indirectly-*
- *Accepts or agrees or offers to accept any gratification from any other person, whether for the benefit of himself or herself or for the benefit of another person; or*
- *Gives or agrees or offers to give to any other person any gratification, whether for the benefit of that other person or for the benefit of another person, in order to act, personally or by influencing another person so to act, in a manner-*
  - *(i) that amounts to the-*
    - *(aa) illegal, dishonest, unauthorised, incomplete, or biased; or*

(bb) misuse or selling of information or material acquired in the course of the exercise, carrying out or performance of any powers, duties or functions arising out of a constitutional, statutory, contractual or any other legal obligation;

(ii) that amounts to-

(aa) the abuse of a position of authority;

(bb) a breach of trust; or

(cc) the violation of a legal duty or a set of rules;

(iii) designed to achieve an unjustified result; or

(iv) that amounts to any other unauthorised or improper inducement to do or not to do anything,

is guilty of the offence of corruption".

Further to this, PRECCA makes mention in Sections 10 – 22 about various matters that would fall under the term of either gratification or corruption or both. The sections are titled as follows:

- *Section 10 : Party to an employment relationship : Unauthorised gratification*
- *Section 11 : Witnesses*
- *Section 12 : Contracts*
- *Section 13 : Tenders*
- *Section 14 : Auctions*
- *Section 15 : Sporting Events*
- *Section 16 : Gambling games / Games of Chance*
- *Section 17 : Acquisition of Private Interest : Public Body*
- *Section 18 : Witnesses : Unacceptable Conduct*
- *Section 19 : Alteration (etc) of Records with intent to defraud/conceal/hinder/obstruct*
- *Section 20 : Accessory liability*
- *Section 21 : Attempt, Conspiracy, Incitement*
- *Section 22 : Regarding Property*

All of these sections should be carefully perused by all people involved in any of the above-mentioned type of areas (especially contracts and tenders).

Penalties

The penalties for people not complying with PRECCA are quite considerable. Mention is made of imposing a "fine equal to five times the gratification involved in the offence'.

Disclosure Requirements

The disclosure of such corruption needs to be performed by "*Any person who holds a position of authority* and who knows or ought reasonably to have known or suspected that any other person has committed-

- an offence under Part 1, 2, 3, or 4, or section 20 or 21 (in so far as it related to the aforementioned offences) or Chapter 2; or
- the offence of theft, fraud, extortion, forgery or uttering a forged document, involving an amount of ***R100 000 or more***, must report such knowledge or suspicion or cause such knowledge or suspicion to be reported to any police official".

"*Person who holds a position of authority*" does relate to a number of people and one should take note if you fall within one of these categories.

- The Director-General or head, or equivalent officer, of a national or provincial department;
- In the case of a municipality, the municipal manager appointed in terms of section 82 of the Local Government: Municipal Structures Act, 1998 (Act No 117 of 1998);
- Any public officer in the Senior Management Service of a public body;
- Any head, rector or principal of a tertiary institution;
- The manager, secretary or a director of a company as defined in the Companies Act, 1973 (Act No 61 of 1973), and includes a member of a close corporation as defined in the Close Corporations Act, 1984 (Act No 69 of 1984);
- The executive manager of any bank or other financial institution;
- Any partner in a partnership;
- Any person who has been appointed as chief executive officer or an equivalent officer of any agency, authority, board, commission, committee, corporation, council, department, entity, financial institution, foundation, fund, institute, service, or any other institution or organisation, whether established by legislation, contract or any other legal means;
- Any other person who is responsible for the overall management and control of the business of an employer; or
- Any person contemplated in paragraph (a) to (i), who has been appointed in an acting or temporary capacity".

Extraterritorial jurisdiction

PRECCA does extend beyond just SA and makes specific reference to extraterritorial jurisdiction, but does list specific requirements for it to be enforced, as listed below.

- *Act affects or is intended to affect a public body, a business or any other person in the Republic;*
- *Person is found to be in South Africa; and*
- *Person is for one or other reason not extradited by South Africa or if there is no application to extradite that person".*

Public Finance Management Act No 1 of 1999

Fraud prevention plans aim to manage the risk of fraud through cost effective use of the control environment, information systems, control procedures and an ethical culture within the department. Each accounting officer must ensure that the fraud prevention plan is completed no later than 31 March 2001.

Local Government: Municipal Finance Management Act No 56 of 2003

No specific mention is made within this act with regards to fraud prevention, but reference is made to financial misconduct and the penalties surrounding them. Furthermore, mention is made of irregular/fruitless and wasteful expenditure amongst other issues.

Conclusion:

Legislative issues are constantly changing and one needs to be fully conversant with its stipulations as it does impact upon your business, irrespective of whether you are a SMME or not. Fraudsters in all their guises do not care much about the laws, just the loopholes which can be exploited.

N. CONCLUSION

In a recent Business Day newspaper article, Provincial governments are responding to President Thabo Mbeki's call to invest in small, medium and micro enterprises (SMMEs) as a platform to create jobs. The following injections and business activities are happening in the provinces both in the formal (f) and informal (inf) businesses:

- **NorthWest:** R68.2 million; 11 000 (f) / 175 000 (inf); ABSA R25 million
- **Gauteng:** Gauteng Enterprise Propeller Agency; R300 million; 199 000 (f) / 616 000 (inf)
- **Limpopo:** Limpopo Development Enterprise; R100 million; 10 000 (f) / 266 000 (inf)
- **Western Cape:** Red Door Initiative; R110 million; 78 000 (f) / 111 000 (inf)
- **Northern Cape:** 5000 (f) / 17 000 (inf); ABSA and FNB working on financial accessibility
- **KwaZulu-Natal:** R300 million; 54 000 (f) / 580 000 (inf)

With this amount of injection in the provinces, government will look to SMME's to ensure that they are aware of their business risks and do not trade recklessly or negligently. Based on this SMME's need to demonstrate good business practice and sense should they require further investment from government. SMME business statistics indicate that 70-80% of start-up businesses fail in the first two years of operation and partnerships formed to start-up or buy businesses do not last more than three years.

What is evident about the success of the SMME business and the relevance to fraud is that if one does not understand the basic principles of business, possess thorough business knowledge and the risks associated with it (of which one key risk is fraud risk), one enters a potentially black hole of risky business which will be short-lived and financially draining.

In majority of businesses it all starts with a plan – a business plan. But it shouldn't stop there; this business plan should include your Fraud Deterrence Strategic Plan (FDSP).

If you fail to plan, you plan to fail.

If you become complacent within your business, the criminals will not be far behind. Like any criminal, the fraudster is generally looking for an easy target. If he runs up against roadblocks, he will try to find another weakness or another victim until he gets what he wants. The criminal will concentrate his efforts to find the one single weakness in your infrastructure that will permit him to widen the crack in the dike of your defences. We should expect no less from him because it is in his best interests to do so. He will not pummel his head against protected walls when he knows that another open entryway is beckoning him.

The technology, the techniques, and the tools exist to defend against, and defeat, fraudsters. There are products on offer to protect against document forgery and counterfeiting, computer viruses, hackers, modem attacks, and all the other tools in the arsenal of the criminal. Given that the technology exists to protect ourselves on a business level, we should try to understand why we remain defenceless. 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** and/or **arrogance.**

On a business level, the danger of procrastination is potentially very dangerous. Procrastination is an addictive drug, and 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 and expenses.

Adequate defences against most frauds are available. Just as the technology for the offensive criminal is cheap and readily available, so the defensive techniques are well known and available for the asking. Technology alone, however, will not solve the underlying ailments affecting us.

Fraud has many faces, and suitably motivated people will invest time studying the way your company operates to commit fraud against it.

What is absolutely necessary is a corporate policy that acknowledges the threat while mapping out a plan for action, combined with regular fraud awareness training, which, in our opinion, is the key to the whole security process. Unless organisations draft an ethics policy, to encompass all the required parameters and which becomes a working corporate policy, fraud will continue to escalate. **"Knowing *what* to do isn't enough – knowledge must be turned into *action* ".**

As you will have seen from this training course, there are solutions to fraud. The bottom line is that it's your money that's at risk, and you now have a choice to make: are you going to be pro-active and seek expert advice, then implement the recommendations, thereby making yourself a hard target, or are you going to be complacent and roll out the red carpet for the criminal?

"In America, the slogan is "ready, fire, aim". In South Africa, our equivalent is "ready, aim, have another conference, aim, have another meeting, aim…" We don't pull the trigger and fire, but that is precisely what South Africans need now – action, not words." Clem Sunter – Home Truths, 1998

NOW would be good time to reconsider your organisation's situation.
Tomorrow may be a large fraud too late!

Frequently Asked Questions

Question 1

OK, I'm convinced that fraud is a serious threat to my organisation. How do I convince my boss to listen to me?

Answer1

This is the question I am asked most often by delegates. As you would have seen from the training course, the majority of organisations simply want to know if the delegate 'enjoyed the course', instead of finding out if something of value was learnt, if the delegate is going to implement what he/she learned, and then find out if the actions implemented actually got the desired results.

The other problem that we must consider is the 'Buyer – Seller' relationship in organisations. The buyer of controls is normally a senior person (director), who tends to have the authority but does not understand the risks. The seller of controls (internal auditor, accountant) understands all the risks but has no authority and has to try and convince the director to follow his/her recommendations. The following outline should help you to get action on your recommendations:

The benefit from anti-fraud work is not in the recommendations made, but in their effective implementation. Important measures of an audit department's effectiveness are the type of issues it tackles and the changes/improvements it is able to effect. In addition, one of an auditor's***** basic objectives is to have his or her work make a difference.

When a recommendation is made to a department, its management is basically responsible for implementing it. But auditors can do a great deal to improve the likelihood that a recommendation will be appropriately implemented. The purpose of this guide is to help auditors get more action and better results from their audit work through the following means:

- **Quality recommendations:** Whether control results are achieved depends on the quality of the recommendation. A recommendation that is not convincing won't be implemented. A recommendation that does not correct the basic cause of a deficiency may not achieve the intended result.
- **Commitment:** When the auditor is committed to the need for action on a recommendation, he/she will do what needs to be done to get it implemented. Without that commitment, a recommendation may not achieve the desired action.
- **Aggressive monitoring and follow-up:** Acceptance of a recommendation does not ensure results; effective implementation does. Continued attention is required until results are achieved.
- **Special attention to key recommendations:** While all recommendations require follow-up, some deal with particularly serious or flagrant matters. They should receive special attention. Auditors should ensure that key recommendations are fairly considered when effective use of the first three principles has not done so. They should reassess strategies to get positive action on their recommendations. Outside intervention should be considered when it would help to get necessary action on key recommendations of great significance.

***** The term 'Auditor' is used generically and can refer to anyone making control recommendations.

Question 2

Why does Fraud Prevention and Detection have to be 'sold' to management?

Answer 2

Management usually does not support fraud prevention and detection for one of several reasons:

- Management's concerns are often elsewhere than audit or fraud. They don't typically understand that fraud is hidden and that losses go undetected without our knowledge. They may also refuse to believe that their own staff is capable of stealing even when studies show that 80% of most frauds involve employees.
- Because of the hidden nature of fraud, managers are reluctant to believe that fraud actually exists. And if one employee is caught committing fraud, management may claim that this is an isolated problem and not worth additional consideration.
- Management may feel that by bringing up the issue will have a negative impact and may alienate the staff. This problem can be addressed by reminding management that the rank-and-file workers appreciate working for an honest, profitable company.

Some of the following suggestions may help in selling fraud prevention to management:

The impact on the bottom line – fraud impacts net sales rand for rand. For example, if a company nets 20% on sales, they must sell 5 items at regular prices to recover losses from the theft of just one item. Fraud can be very expensive.

Computing fraud losses – because fraud is hidden, the auditor can estimate losses:

In the absence of good data, auditors can use the '2% rule' to compute potential losses. This assumes that within a given population of people, at least 2% will steal in quantity. Or put another way, 2% of sales can be reasonably lost to fraud. If this figure seems high remember that 1% of the US population is under the care of criminal courts and these are the ones who are caught, prosecuted and convicted – the 'tip of the iceberg'. Also, the ACFE survey found that the average fraud loss to US organizations per annum is 6% of **turnover**.

If the organization has historical experience with fraud, the figures derived from these past cases can be used to compute potential losses. The problem with this method is that it will probably consistently underestimate losses.

The impact of publicity – many corporate executives are more sensitive to adverse publicity than almost any other issue. Certainly, one way to convince management of the logic of fraud prevention is to point out that negative publicity, even in small doses, can have a devastating impact on the bottom line. This negative impact can be eliminated or reduced by a proactive fraud prevention program.

Between 1996 and 1997, one of South Africa's largest industrial companies detected 3 incidences of management fraud. Over R50 million was stolen of which at least half was recovered and the balance paid out by fidelity insurance – but because of the adverse publicity over R7 BILLION of shareholder wealth has been destroyed!

Remember Barings Bank – the external auditors were sued, staff lost their jobs, and the directors were sued. Fraud is very expensive!

Conclusion

Fraud is a major threat to any business but there are steps that can be taken to minimise the risks. A business that is alert to the risks, that takes steps to put in place appropriate controls and procedures, monitors the operation of these controls and their ongoing effectiveness and maintains an anti-fraud culture, is going to be better placed to deter, prevent, and at worst, detect fraud. Taking the risk of fraud seriously can help protect a business's bottom line, its image and reputation.

Question 3

How do I know I'm making the right decision?

Answer 3

Making decisions is a fundamental life skill. Yet with all the experience we continue to mess up along the way. History is littered with glaring mistakes from poor decision-making. For stakeholders and players in the prevention of crime and its stepchild corporate deviant behaviour, faulty decision-making has been a precursor to corruption crisis in organisations. This renders a new perspective to the idea of getting to the root cause of crime.

For 1000 years of evolution people have continued to make decisions that are beneficial. That is, beneficial to their nearest and dearest and then to others in society and organisations. Only very rarely are they in full possession of enough information to make what an analyst would declare to be the best decision.

Why did Princess Di's driver decide that breakneck speed would be the solution to the Paparazzi in Paris? This speed was made on a foundation of drug abuse earlier in the same day. The outcome was death.

Why did Hansie Cronje decide to pursue match-fixing negotiations that compromised a nation's status internationally, the careers of three players, and then blame Satan?

Why did Hitler change strategy focus to Russia in midwinter in his maniacal desire to rule the World?

Why did Mandela wear silk shirts instead of suits, which would have appeased a white electorate?

Why did Maggie Thatcher bring about her demise at the peak of her career with an unpopular poll tax?

What made Gorbachev pursue Perestroika?

Why did John F. Kennedy secretly contract to build the Berlin Wall with Khrushchev without telling the American or international publics? A national interest decision that he did not dare make public?

Question 4

Why are we so bad at making decisions?

Answer 4

Research says humans make decisions on very limited information. Quite often, these decisions are made only from the information provided by own ears, eyes and sense of smell. Seeing, hearing, touching and smelling gives us a sense of immediacy - of being all-powerful. We tend to have an overwhelming faith in information acquired by our senses rather than the information we read about, or we has been analyzed.

Decision situations vary greatly. The experience of one important decision is not likely to be experienced in the next. What job do I take? What house or car do I buy? What food do I eat today to live longer?

Decisions often have a knee jerk emotional base rather than that of pure logic. A recent Economist survey on 'Why Mergers fail' confirms the emotion driven decisions of CEOs who do not consider the big picture. A wholesome perspective of the big picture does not drive the decisions, but rather personal agendas, which make the act deviant in itself. Not considering the impact of staff that lose their jobs through '*make lean, make mean'* operations.

During this presentation I will use well-known public figures as their activities deviant or otherwise, are easy to trade down and analyze. Too often deviance is not associated with their actions.

Question 5
Can we learn to make better decisions?
Answer 5
We can learn to make better decisions. Ironically we require both skills and competencies depending on the quality of the decision. Understanding the difference between the two is important. A competency for instance is conducted at speed and renders the situation risk averse

SA. Public perspectives

Mbeki makes a decision not to damn Mugabe's land redistribution policy publicly. His value system is questioned. The public wonders whether we are not witnessing true Machiavellinism with sinister potential for white South Africans. Mbeki is denounced. But Mbeki made a decision in the face of the following: national interest knowing that Mugabe was a wild cannon; that Zimbabwe owed S. Africa a great deal of money; that Zimbabwe like South Africa was S.A. trading partner in SADC and that the hip shooting President was capable of deploying menacing army artillery on or own borders.

Decision making problems

Psychoanalyst Twersky identifies a number of decision-making approaches. Three of these are explained in magical thinking, expected utility theory and anchoring:

Magical thinking, where individuals think they have far greater power than they really have. Like Hitler, Louis Luyt in taking on the State President and Cronje – the untouchables. People who fall in love with their own propaganda. Also an investor who buys share that go up and he attributes this improvement on personal wealth to his response of personal inner feelings and skills rather than the vagaries of the Stock Exchange and response to real life events.

Expected Utility Theory: Reeva Forman who took on the Argus and Jani Allen who took on the London Press – on principle. They wanted to be right rather than win the war. They forgot who owned the barrels of ink!

Anchoring: When individuals allow outside factors to influence their decision-making that has no relevance to the subject itself. A number of hijacks in the immediate environment are attributed to the alignment of the stars. Personal success is attributed to *the Age of Aquarius!*

Question 6
What is a recommended Decision-Making approach?
Answer 6
All successful approaches cohesively narrow down the process to logic and an almost mathematical style of thinking rather than emotion alone.

An effective decision making process will fulfil these six criteria:

- It focuses on what is important and practical
- It is logical and consistent
- It acknowledges both subjective and objective elements and blends analytical with intuitive thinking
- It requires only enough information and analysis that is necessary to resolve a particular dilemma
- It encourages and guides the gathering of relevant information and informed opinion
- It is straight forward, reliable, easy to use and flexible

Q & A numbers 3-6 courtesy of the Decision Making Research Institute, which is run by Denise Bjorkman in Sandown Sandton. It is affiliated to the International Federation of Professional Coaches and Mentors of which she is Sub Saharan President. It runs on-going training programmes in the prevention of fraud and corruption.

Today's Decision…

tomorrow's success,
or
tomorrow's fraud?

STATISTIC & ARTICLE SOURCES

American Bankers Association
APACS (Association of Payment & Clearing Services) - UK
Audit Office of NSW - Australia
Association of Certified Fraud Examiners (ACFE) – USA
Banks Automation News
BBA (British Bankers' Association)
Bowman Gilfillan Hayman Godfrey Inc.
Business Against Crime – KwaZulu Natal
Checks & Checking
City of London Police
The Computer Security Institute
'Cooking the Books' – ACFE
Corporate Governance – Tom Wixley
'Dirty Business' by Maurice Punch
Ernst & Young Forensic Accounting – UK, Australia
FBI
Federal Deposit Insurance Corporation
'Forensic Auditing & Forensic Accounting' by G. Jack Bologna and Robert J. Lindquist
Frank W. Abagnale
'Frankensteins of Fraud' by Joseph T. Wells
Fraud – "Bringing Light to the Dark Side of Business" by W.S.Albrecht
'Fraud Detection' by David Coderre
'Fraud Examination for Managers & Auditors' by J.C. Robertson
'Fraud Watch' by Ian Huntington & David Davies
GAO (the General Accounting Office – USA)
'How to Detect & Prevent Financial Statement Fraud' - ACFE
Ian Melamed
'Information Warfare' by Winn Schwartau
IIA (Institute of Internal Auditors)
Interpol
ISS (Institute for Security Studies)
ISR ('International Security Review' - UK)
Kevin Daly – S.A. Banking Council
Leigh-Marden (Pty) Ltd. - Australia
Maxima Group Plc - UK
Neville Phillips – Standard Bank legal department
Nigel Payne – Transnet Internal Audit
'Occupational Fraud & Abuse' by Joseph T. Wells
'Other Peoples Money' - ACFE
Royal Canadian Mounted Police
Scientific Document Services (Pty) Ltd. - Australia
SensePost
Transparency International
US Secret Service

ANNEXURES

Annexure A:

FRAUD CHECK LIST FOR BUSINESS OWNERS / MANAGERS

Does your business:

- Treat fraud as a business risk?
- Identify the types of fraud to which it is most exposed?
- Ensure that at least one person or department is specifically identified as responsible for managing fraud risk?
- Make clear to all employees that fraud prevention and detection is the responsibility of everyone in the business?
- Have, and actively promote, a fraud policy statement?
- Have a strategy and procedures for managing the prevention, detection, investigation and prosecution of fraud?
- Have a fraud prevention education / training programme?
- Have a plan of action in the event that a fraud is detected?
- Have a clear whistle-blowing policy?
- Have recruitment and ongoing personnel policies that address the risk of fraud?
- Check that your fraud policies and procedures are complied with?
- Ensure that your fraud policies and procedures are regularly reviewed?

If you answered 'NO' to any of the above, you may have vulnerability within your organisation that could expose you to fraudulent activity and behaviour.

Annexure B:

KEY ELEMENTS OF A FRAUD PREVENTION STRATEGY:

- Identifying the areas within the business most vulnerable to the risk of fraud
- Establishing what processes are in place already
- Identifying extra or alternative controls needed to reduce the risk
- Introducing the extra or alternative controls
- Monitoring the controls to check that they are in operation
- Regularly assessing the effectiveness of the controls, in particular to take account of the changing circumstances in the organisation.
- Ensuring that your strategy and procedures are workable and practical; supported by appropriate resources and regularly reviewed.

The fraud prevention strategy covers one-third of the fraud deterrence strategic plan. The fraud detection and investigation strategy forms the other two-thirds. Without an effective fraud prevention component, the possibility of preventing fraud before it occurs is limited to non-existent at best. Focussing on the above-mentioned elements (of a fraud prevention strategy) creates a more concentrated approach in dealing with fraud before any potential loss is suffered.

Annexure C:

ASSESSING FINANCIAL STATEMENT FRAUD:

In assessing risk of financial statement fraud, the business owner / internal auditor should complete the following *Questionnaire for Assessing Risk of Fraudulent Financial Reporting.*

The Control Environment	**Yes**	**No**
1. Are the internal controls that govern financial reporting adequate?		
2. Is the degree of emphasis on reaching earnings forecasts, budgeted targets, or the price of the company's stock, excessive?		
3. Is the emphasis on performance in management's compensation plans excessive, with bonuses tied to reported earnings or stock prices?		
4. Is there excessive turnover in key personnel of internal audit staff, internal accounting staff, or in-house counsel?		
5. Is the turnover in independent accountants, lawyers, and banks excessive?		
6. Is the organizational structure so complex as to be vulnerable to fraudulent practices?		
7. Is management's attitude towards the selection of accounting principles and policies aggressive?		
8. Is the Financial Director aggressive in applying accounting principles & policies to achieve top management's goals in earnings & revenues?		
9. Has top management abdicated its control over lower divisions or departments to the managers of those departments?		
10. Is top management so dominant that the Board of Directors, the Audit Committee, or the Internal Audit department are ineffective?		
11. Is the accounting department weak?		
12. Is the internal audit staff truly independent?		
13. Are the budget and forecasts realistic as compared to actual results?		
14. Does the company personnel department do a thorough background check on key employees when hiring them?		
15. Does the company have a written code of corporate conduct?		
16. Does management adhere to the code of corporate conduct?		

The Control Environment	**Yes**	**No**
17. Does management try to comply with governmental rules and regulations that affect the company, including, but not limited to, income tax rules and regulations?		
18. Does top management protect "whistle blowers" when they blow the whistle on violations of the corporate code of conduct?		
Financial Characteristics		
19. Is the company suffering from liquidity problems?		
20. Are operating earnings significantly more than cash flow from operations?		
21. Is the trend of operating earnings or operating cash flow downward?		
22. Are sales and revenues down?		
23. Has the quality of receivables deteriorated due to higher credit risks or slower paying customers?		
24. Has the quality of operating revenue deteriorated? (Consider liberalized credit policies, unusual discount and payment programs, declining sales backlog)		
25. Are company's reserves for losses (bad debts, loans) adequate?		
26. Is the company compelled to borrow because of deteriorating earnings or operating cash flow?		
27. Is the company close to violating restrictive debt covenants?		
28. Are the downward trends worse than the industry's downward trend?		
Operations		
29. Are there any indications that inventories are increasing beyond normal ratios to cost of sales? (Produces attempts to load sales, ship without orders, ship "in place," ship on consignment, ship with unrestricted right of return)		
30. Are there any new types of sales incentive programs that could lead to the abuses listed in item 29?		
31. Does a present or planned computer installation allow management or key employees to commit fraudulent acts through the computer system?		
32. Are there any planned, pending, or probable mergers or acquisitions in which stock price is a factor?		
33. Have customer complaints or sales returns increased over historical averages?		

34. Are there any related party transactions that are not based on *objective determinations independent of the parties?*		
35. Is the company dependent on a key customer or a key supplier?		
Individual Management Characteristics		
36. Is there any history of- a. Criminal convictions? b. Litigation involving allegations of fraud? c. Civil proceedings? d. Tax fraud proceedings?		
37. Are there any significant personal financial difficulties? (High personal debts, inadequate income, stock speculation, gambling, drugs, or alcohol)		
38. Is there any significant instability in personal life? (Divorces, extramarital escapade "high flyer")		
39. Is there any resentment against the company for alleged unfair treatment?		
40. Are there any manifestations of "win at any cost," "be top dog," "the Emperor," "this is *MY COMPANY"?*		
Accounting Policies and Procedures		
41. Are there transactions involving unsettled, difficult, or controversial accounting issues?		
42. Are there assets with difficult valuation problems? (Excessive inventories, private placement securities, contract rights acquired, or intangibles)		
43. Are there transactions or unusual adjustments completed at or made effective just before the end of a quarter or a year-end?		
44. Are the company's procedures for identifying and recording related party transactions adequate?		
45. Are the company's accounting records and management reporting system current, modern, well-designed, and well-organized with an up-to-date accounting manual that gives effect to the most recent accounting standards, policies, and principles?		
46. Is the company's application of GAAP to its accounting liberal, and have there been disputes between the auditors and the company about the application of those principles?		
47. Do the audit committee and the Board of Directors get financial statements well in advance of meetings?		
Industry Conditions		
48. Is the company's performance contrary to cyclical, seasonal, or long-term conditions in its industry? (e.g., industry sales down, company up; industry earnings down, company up; industry declining, company expanding; industry conditions adverse, company improving)		

Business Environment		
49. Are there any contests for ownership or control of the company?		
50. Are any of the principal products of the company suffering from obsolescence, customer disinterest, or style change?		
Legal and Regulatory Considerations		
51. Are there any licenses and agreements that contain performance requirements that the company is not meeting?		
Legal and Regulatory Considerations	***Yes***	No
52. Are there any new tax laws or interpretations that put pressure on the company's earnings?		
53. Has any regulatory agency imposed financial restrictions on the company that it must meet if it is to continue in business?		
54. Are there any new governmental rules or regulations that change the manner in which the company must conduct its financial and business affairs?		

Annexure D:

MOST COMMON METHODS OF COMMITING FRAUD IN OWNER MANAGED EMERGING BUSINESSES:

Debtor Fraud

Redirecting and stealing debtor remittances is a common method of fraud in owner managed emerging businesses. It occurs primarily because of limited controls and segregation of tasks among finance staff. This type of fraud often goes undetected for some time and if given the right environment can remain undetected.

How?

In most situations staff with access to debtors' receipts, banking and the debtors system commit the fraud. Most organisations believe banking systems protect them. However, banks do not and cannot have systems to detect all clever deception. Despite common perception, banks do not review every cheque for signatures or the correct payee of each cheque.

For example:

- Finance manager of company, First Pty Ltd, collects cheques or opens mail.
- Has previously set up a company called Frist Pty Ltd.
- Opens up bank account in company name.
- Deposits stolen company cheques in the name of First Pty Ltd into Frist Pty Ltd bank account – Bank officer does not see the subtle differences in the company name and processes.
- The finance manager, who also controls the debtors, can either continue to re-age the fictitious debtors balance or, if the performance of the company is strong enough, he/she could systematically write off the fictitious balance to an under budget expense account, so as not to raise the suspicion of anyone who scrutinises the financial results.
- The finance manager could continue this process, and even begin to budget for the amounts he intends to steal during the year.
- In this example the defalcation could proceed for many years without being identified and could, depending on the size of the organisation, drain significant amounts of cash from the business and shareholders and may even contribute to financial failure.

Recommended actions

- The following examples of generic recommendations provide a framework to reduce the risk of fraud involving debtors.
- Ensure that debtors and banking functions are performed by different personnel and tasks are periodically reviewed to ensure compliance.
- Try to eliminate unsupervised long periods of pattern behaviour that allows individuals to circumvent controls.
- Ensure random review of senior personnel and critical controls and processes. Am element of surprise will ensure patterns are not created.
- Ensure the debtors system has strong controls over the processing manual journal entries.
- Periodically review cheques received to the daily banking summary.
- Be involved in the financial statements and understand how they link in with your business fundamentals.

The General Ledger Mess

The general ledger mess is far too common among emerging or owner managed businesses. While sometimes is innocent, the reason can be to camouflage fraud. This type of fraud often occurs when the following factors are present:

- Finance manager has total autonomy in relation to finance matters, and often the finance manager has a broader "general manager" role.
- Finance department is understaffed, and may not have the required skill levels and experience.
- CEO has very little involvement with finance other than review of monthly results.
- Monthly financial results are prepared as spreadsheets outside the general ledger and therefore may bear no resemblance to what the general ledger reflects.
- Monthly reconciliations are not performed and there are very little controls.
- Auditors are often smaller firms who undertake substantive audit procedures around information provided by finance manager. No information system work is undertaken as the finance manager insists the system is corrupt and continues to produce errant journal entries.
- No internal audit role in the organisation.

How?

The general ledger mess can be a camouflage designed to confuse and frustrate anyone who stumbles across any anomalies in the results of the business. The finance manager creates a complicated web of unusual journal entries to asset, liability and suspense accounts to provide the perfect platform to write cheques to his/her benefit.

- The finance manager then prepares a set of financial statements on spreadsheets, which reflects what the audience expects to see, and therefore raises few, if any, questions. This type of fraud can, for years, continue undetected, particularly when the business is doing well, because expectations of what is "normal" have been manipulated over time.
- In some instances the finance manager will write cheques in favour of himself, fictitious vendors or related parties. The cheque will be coded to stock or another general ledger asset code so that the financial result does not raise any concerns or suspicions. Under scrutiny, the finance manager steers the enquirer away from the general ledger (on the basis that it has been corrupted), to his/her created financial statements and fictitious reconciliations.
- The one key ingredient in this type of fraud is that one person has total autonomy over the finance function, and has the necessary authorisation to manipulate controls and processes.

Recommended actions

Ensure random verification of the key functions:

- Bank reconciliation
- General ledger reconciliations
- Ensure that on a random basis the complete audit trail for raising of cheques is verified and traced.
- Ensure that the CEO or chairman meets separately with auditors to understand the scope of audit and to ask questions regarding the quality of the information.
- Do not allow any one person to have total unsupervised autonomy over any function.

Fictitious Invoices

The raising of fictitious invoices is also extremely common, and can originate at any point in the organisation. It is common in smaller organisations for the perpetrator to be within the finance function, as the individual has the opportunity to camouflage the crime by manipulating budgets to allow for the theft of funds.

The fictitious invoices are often raised as suppliers of either goods and services and the fraud is again usually committed by an individual in authority, who can circumvent any controls.

For example

- Procurement manager seeks to set up Multiplus Pty Ltd as a vendor, however uses his authority and influence to circumvent the usual vendor verification process.
- Procurement manager subsequently raises fictitious invoices with fictitious purchase order and goods inward dockets.
- Invoices are duly processed for payment and goods recorded as stock.
- Procurement Manager uses authority to change goods outward documentation to record Multiplus stock code, for a sale to ensure stock of Multiplus in stock ledger is reduced.
- Upon stocktake there is a book to physical stock discrepancy in the correct stock that was delivered, and the error is duly written off as a stock loss.
- Each step in the fraud has been undertaken by using the power of authority or influence.
- The same process can occur within the Finance or other departments for fictitious goods or services.

Recommended actions

- The most important way of preventing this type of fraud is to establish a culture within the organisation of reporting breaches in processes or controls. Creating this culture does not happen overnight, but is an ongoing process to not only minimise fraud from occurring but to protect the innocent employees from the devastation fraud leaves behind.
- Perform random reviews to ensure adherence to written processes and procedures.
- Periodically perform a vendor audit. Interrogate the payments module of the IT system, listing all payments made during a period by vendor and auditing who the vendor is and what they supply. You may even make a phone call to the vendor, if they are not known to you.
- Implement random spontaneous stock cycle counts.

Other common forms of fraud

The following examples show the many ways in which fraud can affect owner managed or emerging growth companies:

- Drawing of cheques in personal name and altering records to reflect a vendor name.
- Pilferage of stock for re-sale.
- Credit card reimbursement for private expenditure.
- Foreign exchange “gambling” for personal gain.
- Kick backs from preferred suppliers at inflated prices.
- Theft and manipulation of social club and petty cash monies.
- Purchase of private capital items (TVs, DVD players etc.) recorded as fixed assets in the organisation.
- Payroll – fictitious employees or duplicate payments or allowances.

Annexure E:

QUICK METHOD TO IDENTIFY POSSIBLE 'HOTSPOTS' IN YOUR BUSINESS:

In a SMME environment, due to personnel shortages or financial considerations, numerous functions are performed by the same person. Although this might be more due to practical reasons, this does place the business at risk due to no segregation of duties across specific processes or sub-processes.

One of the quick ways in which one can see who is involved in several of these key processes or sub-processes is to complete the table below. Fill in the employees details horizontally and document the various processes in the business vertically. Once this is complete, 'tick' off which employees are involved in the various processes.

Your table will now depict a complete view of your business and who is involved in various processes. This now provides you with possible hotspot areas where only one person appears to be involved and as such enables you to start to contemplate how (if possible and practical) one can rotate personnel around to create more adequate segregation of duties.

	Employee 1	**Employee 2**	**Employee 3**	**Employee 4**	**Employee 5**	**Employee 6**	Etc.
Process 1							
Sub Process 1							
Sub Process 2							
Process 2							
Sub Process 1							
Sub Process 2							
Process 3							
Sub Process 1							
Sub Process 2							
Process 4							
Sub Process 1							
Sub Process 2							
Process 5							
Sub Process 1							
Sub Process 2							
Process 6							
Sub Process 1							
Sub Process 2							
Etc.							

Annexure F:

FRAUD DETERRENCE STRATEGIC PLA N ‘TAKE-BACK’ DOCUMENT THAT WILL ENABLE YOU TO START DEVELOPING YOUR VERY OWN

Fraud Deterrence Strategic Plan

A working living guide to limit your current exposure to Fraud

FRAUD DETERRENCE STRATEGIC PLAN

Background:
The purpose of this Fraud Deterrence Strategic Plan (FDSP) is to enable you to capture your thoughts, ideas, suggestions, solutions, concerns, etc as you experience the learnings throughout the duration of this workshop.

We have provided you with a framework to start to develop a 'pathway' to gain a more accurate status of your (or other) organisations 'fraud health'. By populating this document, you will be placed in a more informed position of the potential fraud risk indicators that could be facing your organisation. Furthermore, with this process being set in motion during this workshop, it enables you to start to develop possible solutions to prevent or detect these types of fraud risks.

This is a working document and should not be seen as a 'one-size fits all' approach. It is always recommended to involve key personnel from within your organisation to co-develop this FDSP with you. Additionally, it would be advisable to consult with knowledgeable Fraud Prevention experts who have experience in developing such plans, prior to embarking on a fully-fledged implementation of the FDSP.

Information combination is vital:
In your formulation of the FDSP, it is imperative to understand that it is just as important to know as much about your organisation and how it works as it does to knowing as much about fraud. In essence, there are three parts to the FDSP, namely:

- Your knowledge of your organisation (the 'information pack' that you need to complete as you develop your FDSP)
- Your knowledge of occupational fraud and abuse (and how it can impact on you and your organisations performance)
- Taking the knowledge of your organisation and occupational fraud and abuse and incorporating this into a working document that enables you to formulate a FDSP that will work for your organisation

Remember, each organisation is unique, so although there are certain parameters / guidelines that we will be providing, these may or may not be appropriate for your organisation. It is always advisable to be more comprehensive in your development of the FDSP, instead of limiting your FDSP based on certain organisational constraints or factors.

Work in progress
The FDSP and this workshop is a jumpstart to get you and your organisation thinking about fraud and the possibilities of it occurring on your doorstep. It is a working document that needs to be constantly worked on, reviewed, adjusted, re-implemented (where appropriate) and constantly monitored.

Remember, what you cannot monitor, you cannot measure. Hence, the reason why the FDSP is important as it provides you and your organisation with a tool that can be used to measure the adequacy and effectiveness of your FDSP initiatives and whether those objectives are being met.

Document Compilation:
In the development of this document, you will have to start to think differently about your organisation – think like a fraudster! Yes, when you start to think differently, it creates greater potential areas of fraud exposure that were not necessarily identified before.

To get you going, a section titled **environment scan** has been provided to get you into the ‘fraud zone’. This will start to focus your energies on the end-result, namely being able to understand your business and the potential impacts fraud may have on it, should no effective action be implemented to prevent it from occurring.

Thereafter, we have provided you with the sections that will be covered during the workshop with page references. Please use these pages to jot down memory-joggers to include in your FDP. Remember, the more comprehensive your FDSP is, the greater the degree of success in minimising potential fraud exposure in identified risk areas.

Last thoughts:
This is not a race, but a journey to develop the ***most effective and sustainable*** Fraud Deterrence Strategic Plan for **YOU** and your company. You have been afforded the time to attend this workshop and gain valuable insights into the ‘fraud zone’, so take your time, absorb the information, but don’t lose your thoughts, put them down.

It’s all about awareness. Become aware and share.

ENVIRONMENT SCAN

Mission / Vision	- What is your company's mission? - What drives them? - What are the strategies / objectives to achieve this?
Values	- What are your company values? - Do you know what they mean? - Do others know what they mean? - How do these values get exhibited? (behaviours)
Financial Statements	- What does your Balance Sheet look like? - What is your Sales / Turnover figure? - Any Corporate Governance statements in the notes
Industry	- Is your organisation a Subsidiary or wholly owned? - Are you regulation-intensive? - Is your industry problematic? - Is your industry labour-intensive? - Are you IT-dependant? - Industry dishonest, cutthroat or corrupt? - Other
Employees / Employee Make-Up %	- How many employees? - Where are they located locally, globally, etc? - Admin staff %? - Management %? (lower to middle to exec) - Sales staff %? (if any) - Years service (average) - Age (average)? - Young vs old - Permanent / Temporary %? - Contractor staff %? (outsourced services)
Organisation policies (what policies do you have in place)	- Money laundering - Ethics - Fraud - Information Protection / Confidentiality - Conflict of interest - Gifts - Other
Culture	- What culture exists in your organisation? - Does the same culture permeate in your area? - Top-Down or Bottom-Up or Inclusive vs Exclusive - Performance driven / sales driven?
Streamlining / Changes	- Process / Technology / Industry / Legislative changes - Management changes - Restructuring / redevelopment
Fraud reality	- Possible areas of fraud in your organisation? - Recent risk assessments – high risk areas? - Collusion / Kickbacks / Unfair practices, etc

MY ORGANISATION

Mission / Vision:
Values:
Financial Statements:
Industry:
Employees / Employee Make-Up:
Policies:
Culture:
Streamlining / Changes:
Fraud Reality:

INTRODUCTION
Page 4 – 13

CORPORATE GOVERNANCE
Page 14 – 25

CORRUPTION
Page 26 – 40

ASSET MISAPPROPRIATION
Page 41-47

FRAUDULENT FINANCIAL STATEMENTS

Page 48-59

ORGANISED CRIME
Page 60-63

COMPUTER CRIME
Page 64-69

REDUCING YOUR FRAUD RISK

- *PREVENTION (Page 70 - 89)*
- *DETECTION / INVESTIGATION (Page 90 – 99)*

APPLICABLE LEGISLATION

Page 100 - 103

CONCLUSION
Page 104

CHALLENGES / WAY FORWARD

What do you believe are <u>concerns</u> for your organisation?

- …
- …
- …
- …
- …
- …
- …
- …

What do you believe you can have an <u>influence</u> over?

- …
- …
- …
- …
- …
- …
- …
- …
- …
- …

What do you believe are <u>possible obstacles / challenges</u> for you in implementing a FDSP in your organisation?

- …
- …
- …
- …
- …
- …
- …

Write down three (3) positive affirmations about what you can do to enhance your organisations ability to prevent or detect fraud from occurring.

1.

2.

3.