

Fraud

A guide to its prevention,
detection and investigation

Fraud in the Australian context

Corporate fraud is a persistent fact of business life, affecting businesses of all sizes and across all industries. Consider the following recent statistics:

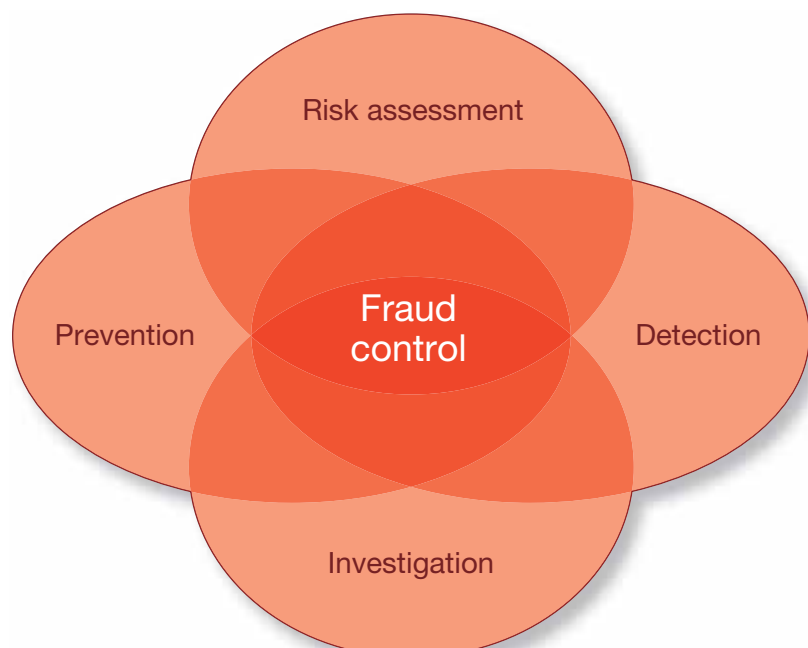
- 49.5% of Australian businesses suffered some form of fraud between 2005 and 2007 (*PricewaterhouseCoopers' Economic Crime Survey 2007*)
- Fraud costs Australian business and government \$5.8 billion a year – one-third of the total cost of all crime in Australia (Australian Institute of Criminology's 2003 report, *Counting the costs of crime in Australia*)
- 21.4% of Australian respondents suffered losses in excess of \$1 million between 2005 and 2007 (*PricewaterhouseCoopers' Economic Crime Survey 2007*).

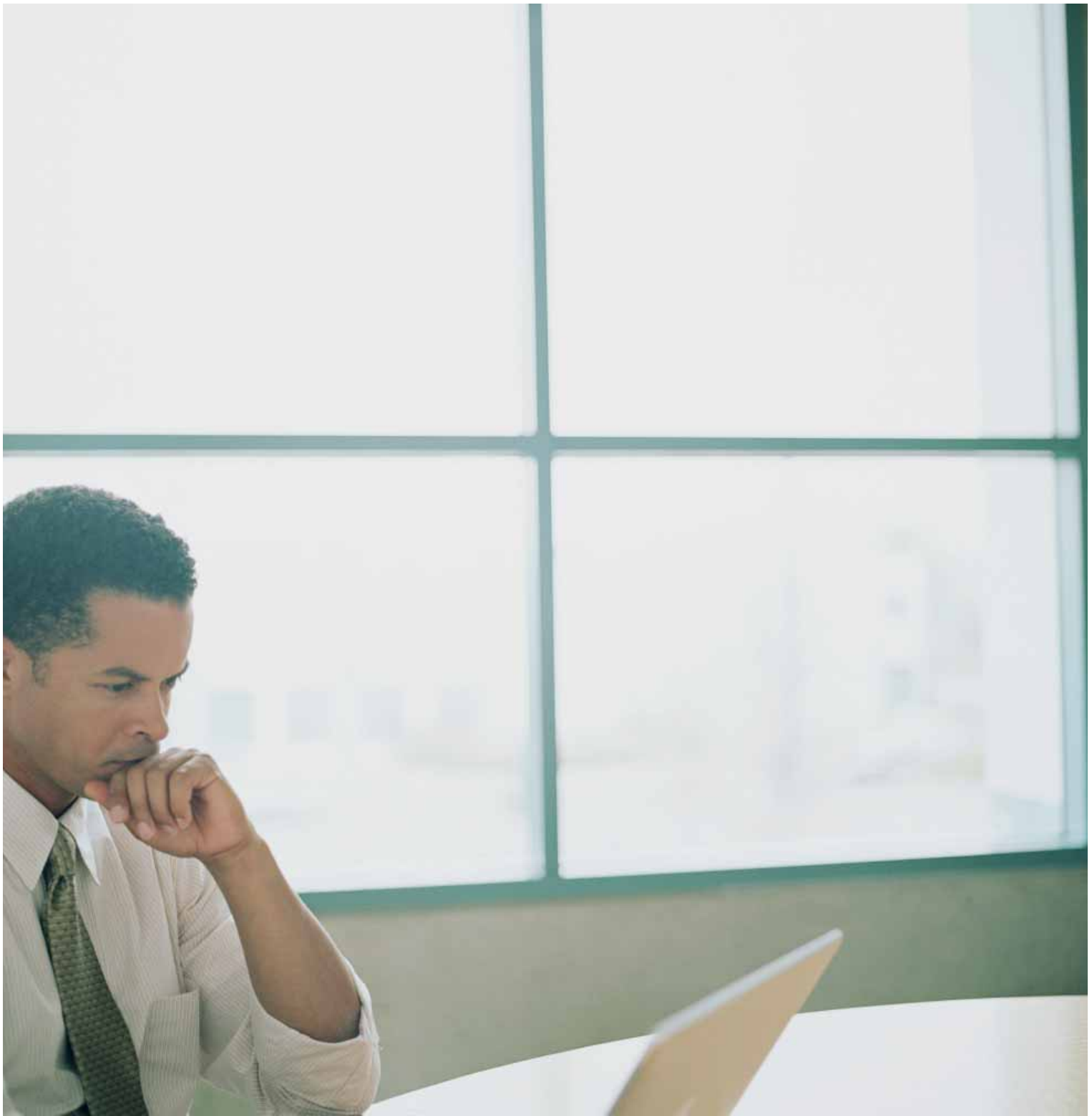
While there is no foolproof method of preventing fraud, the risk can be minimised by taking a systematic and considered approach to its management.

For most organisations, internal fraud (fraud committed by an organisation's employees or officers) is its greatest risk. In fact, the PricewaterhouseCoopers' *Economic Crime Survey 2007* identified that 71.4% of Australian fraud was committed by internal perpetrators.

Therefore this guide is primarily directed toward the mitigation of internal fraud, even though many of the methods described can be used to mitigate external fraud.

The guide will take you on the iterative journey of fraud risk management, providing a basic summary of better practice techniques in fraud prevention, detection and investigation.





While there is no foolproof method of preventing fraud, certain fraud prevention techniques have proven to be successful.

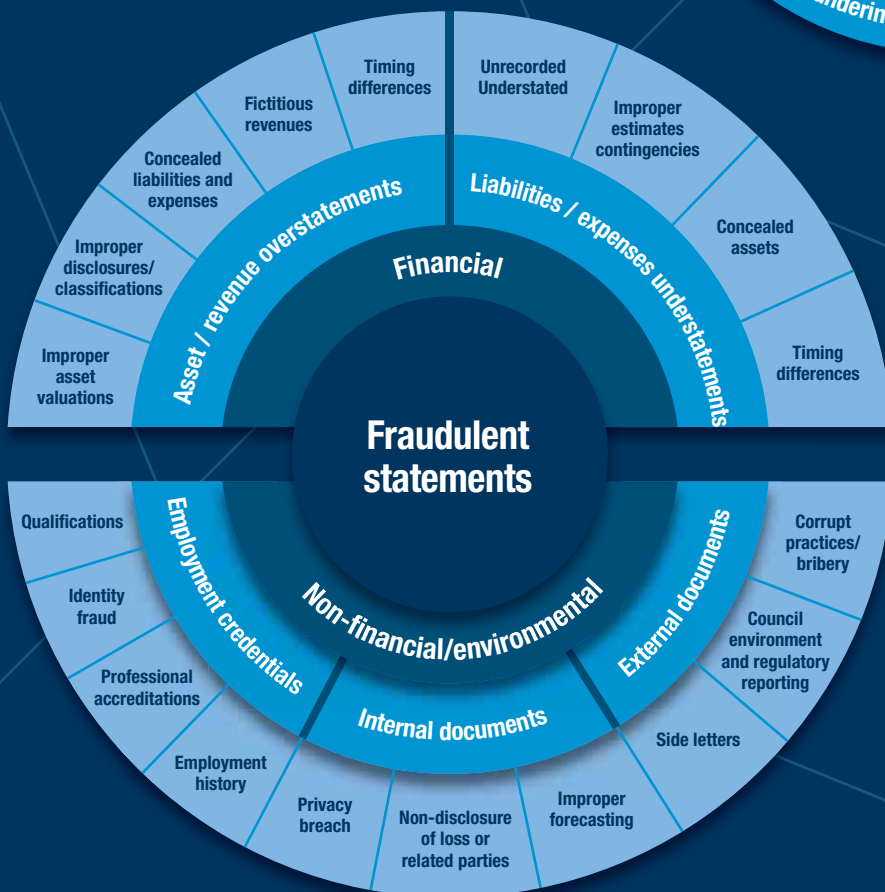
Contents

Introduction	4
1 ■ Fraud risk management	7
How to establish a robust framework	
2 ■ Fraud prevention techniques	13
Some easy-to-implement fraud prevention techniques	
3 ■ Proactive fraud detection	21
Making fraud detection part of business-as-usual	
4 ■ Effective fraud investigation	27
A step-by-step plan	
5 ■ Electronic investigations	35
What if there's no paper trail?	
6 ■ Financial statement misrepresentation	39
Do your numbers lie?	

The web of deceit

"O, what a tangled web we weave when first we practice to deceive!"
 - Sir Walter Scott -



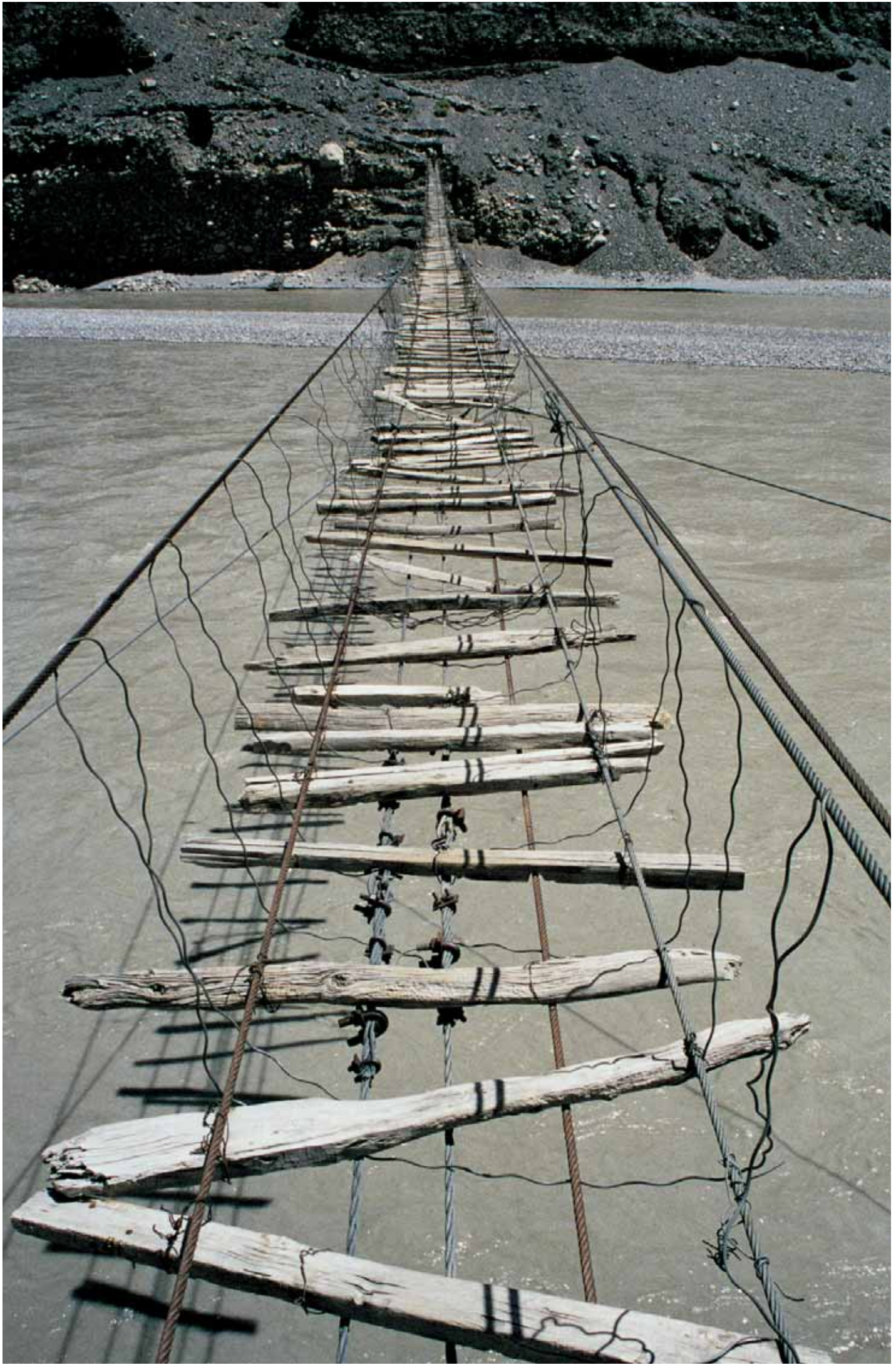


The 'web of deceit' – also known as the Fraud Tree – is adapted from a uniform occupational fraud classification system developed by the United States based Association of Certified Fraud Examiners.

Areas of risk and fraudulent schemes are grouped under the broad categories of asset misappropriation, fraudulent statements and corruption.

It is important when investigating incidents of fraud to remember the concept of the web. This helps remove mental blinkers and reminds the investigator to consider all potential aspects of a perpetrator's fraudulent activities.

In many cases perpetrators will use several different fraudulent schemes that are interconnected. For example, invoicing schemes will often require the perpetrator to create false suppliers and then cover their tracks by creating false accounting records. These have a direct impact on an organisation's financial statements.



Fraud risk management

How to establish a robust framework

1

Fraud and poor governance are serious risks for all organisations. High-profile cases in recent years have shown that dishonest behaviour not only undermines profits, operating efficiencies and reliability, but can severely damage an organisation's reputation.



As a result of fraud-related collapses, governments around the world have undertaken regulatory initiatives in the fraud area. These include rules under the Sarbanes-Oxley Act in the US and the Corporate Law Economic Reform Program (CLERP 9) in Australia.

Also, Australian Auditing Standard (ASA) 240: *The Auditor's Responsibility to Consider Fraud in an Audit of a Financial Report* requires greater:

- transparency in corporate accounting and reporting
- accountability, by making board members and executives personally responsible for financial reports.

A fraud risk management framework

A fraud risk management framework is an essential element in meeting these corporate responsibilities of transparency and accountability. Developing such a framework is a complex task that requires an understanding of Australian Standard (AS) 8001-2003: *Fraud and Corruption Control*.

An organisation must ensure this risk management framework effectively minimises fraud risk across all its operations, while at the same time having the flexibility to adapt to change.

A fraud risk management framework should include the following:

1. Identify areas of high risk

Identifying high fraud risk areas is the first substantive step in dealing with the problem. This must be done before any further analysis and assessment can be undertaken. It is important that risk identification is not confined to financial risks – for some fraud such as cyber crime and information theft, damage to reputation is a key consideration.

2. Assess the risks

Once an organisation has identified its own risk areas, a fraud risk assessment covering all relevant areas of operation can provide the platform for a framework and strategy for a sustainable, long-term monitoring and review process.

3. Involve all staff

In order to capture fraud risk information from all staff, an electronic survey tool should be considered. This can be used across the organisation, or at the business unit or product-specific level. Electronic surveys have the following benefits:

- they greatly assist in lifting levels of fraud risk awareness among staff
- they increase understanding of the effectiveness of the organisation's existing risk management framework, and its capacity to prevent and detect fraud
- they can be used to validate identified fraud risks inherent in specific business units and/or products
- they give staff the opportunity to report known or alleged fraudulent activity.

Conducting a fraud risk assessment

Fraud risk assessment involves a significant commitment by management and staff and should be directed or managed by people, whether staff or consultants, with fraud risk expertise. Once the assessment has been completed effectively, management will be in a position to more adequately prevent fraud against their organisation.

Australian Standard AS 8001-2003 is a good guide to undertaking a fraud risk assessment. It adopts the process outlined in the Australian/New Zealand Standard, AS/NZS 4360: 2004 *Risk Management*: The steps include:

- establishing the context
- identifying the risks
- analysing the risks
- evaluating the risks
- treating those unacceptable risks.

Throughout this process the analyst should continually communicate, consult, monitor and review.

A typical risk assessment will involve a physical inspection of important sites, detailed examination of corporate policies and procedures, interviews with key employees, and examinations of accounting records, computer systems and corporate documentation.

The assessment should include management workshops and brainstorming of 'what if' fraud scenarios. Reviews should focus not only on areas of potential financial loss, but also on non-financial aspects such as intellectual property loss and security. Without such a review,

it is impossible to identify if current procedures and controls are adequate or effective.

Common risk areas

Areas of fraud risk vary from industry to industry and from organisation to organisation. However, six key areas of risk apply to most organisations:

1. Purchasing and payroll
2. Sales and inventory
3. Cash and cheques
4. Physical security
5. Piracy, intellectual property and confidential information
6. Information technology.

1. Purchasing and payroll

Payment fraud, including purchasing, payroll and expense reimbursement fraud, is likely to affect most organisations at some stage. The opportunities for fraud in these areas are high, as they are the main areas where funds legitimately 'leave' an organisation.

Fraudulent transactions can be easily concealed in these outward fund flows. Recent developments in the electronic processing of such payments has increased the risk, and led to new fraud methodologies involving the manipulation of payment systems and master files.

Purchasing fraud is usually perpetrated in one of three ways:

1. kickbacks or bribes are paid to purchasing decision-makers in exchange for supply contracts or uncommercial deals
2. 'false invoices', or invoices from organisations or individuals connected to the purchasing decision-makers, are created and paid
3. purchasing and payment systems and master files (particularly bank account fields)

are manipulated to facilitate fraudulent payments.

Fraudulent payment schemes can be sophisticated and difficult to detect, and such schemes can operate for years before they are discovered.

Fraud indicators include:

- employees and suppliers sharing a bank account
- unrelated employees sharing bank accounts
- duplicate invoices from the same

Case study: Purchasing fraud

A finance director of an Australian parts supply organisation resigned suddenly, citing personal reasons. His actions were then reviewed to determine whether he had acted against the interests of the organisation.

A review of the organisation's supplier master files using an automated fraud detection program revealed the 'bank account' field had been altered for several of the organisation's suppliers. Bank account numbers had been replaced with a common bank account number, and several transactions processed into this account. The account number was traced to the former finance director.

supplier

- excessive employee overtime.

2. Sales and inventory

Sales, debtors and inventory fraud are often closely related. Typical frauds include the following:

- theft of warehoused or floor inventory or diversion of inventory in transit
- unrecorded or understated sales and theft or skimming of cash collections
- unauthorised award of credit notes or credit on account, often through the corruption of an employee

- fictitious sales and corresponding accounts receivable to facilitate commission or similar sales-based payments
- receivable write-off and lapping schemes
- false cancellation or voiding of sale transactions
- unauthorised, fictitious or multiple refunds to customers
- excessive discounting on the supply of goods and services in return for 'kickbacks' (relatively common, particularly in Asia).

Sales frauds are often linked to inventory frauds, where stock is stolen using false sales invoices that are subsequently cancelled or credited by authorised sales staff.

Fraud indicators include:

- sales in one period reversed in the next period
- negative inventory entries
- unauthorised bad debt write-offs.

Case study: Sales and inventory fraud

The sales director of an electronic product manufacturer resigned from his position when confronted with irregularities in sales figures.

An investigation discovered that a significant proportion of sales invoiced to particular suppliers had been falsely created, allowing the misappropriation of inventory from the warehouse.

The fraudulent sales invoices were later credited by the sales director as 'non-inventory return credits'. The inventory itself had been collected by an associate of the sales director, and the sale proceeds shared between them.

3. Cash and cheques

Most organisations have procedures to safeguard cash, yet those procedures are often ignored where cheques are concerned.

Despite a reduction in cheque usage following the transition to electronic fund transfer payments, misappropriation of cheque receipts and cheque payments remains a problem. Most cheque theft occurs within the postal system. However, larger-scale cheque fraud can also occur inside organisations where bank reconciliation processes are weak and there is inadequate segregation of duties.

Case study:
Cheque misappropriation and expense fraud

The finance director of a large, fast growing services organisation found the combination of trusting senior management, poor internal controls and readily accessible funds too tempting. Over a period of several years, he defrauded the organisation of over \$5 million, mostly by purchasing bank cheques using the organisation's funds.

The finance director had sole responsibility for completing bank reconciliations which were falsified and often destroyed. The fraudulent transactions were able to be hidden as unreconciled items due to the existence of high funds transfer volumes within the organisation's bank accounts.

4. Physical security

The PricewaterhouseCoopers *Economic Crime Survey 2007* identified asset misappropriation as the highest risk category for Australia, representing 37.1% of economic crime reported. Although organisations often create and maintain a physical security environment, the controls over access to cash, inventory

and other assets are rarely adequate.

This can lead to large-scale, organised fraud schemes through the theft of inventory, cash and other assets.

A major aspect of any fraud risk management activity will need to be an assessment of the physical security of an organisation's assets.

Case study:
Unauthorised removal of corporate information

A senior manager of an electrical components organisation entered into a contract with an overseas manufacturer to produce identical components for his employers. He subsequently created his own business, resigned from his position and set up in competition. As a result of concerns about the loss of customers, an investigation was initiated.

This investigation established that the senior manager had managed to access a database he was not authorised to enter, and had obtained electronic copies of the complete customer list, product price list and technical information prior to his resignation. This had enabled him to target the organisation's customers and offer cheaper prices. His actions were in breach of the anti-competitive clause in his contract.

5. Piracy, intellectual property and confidential information

Product piracy is one of the major economic crimes facing manufacturers and distributors of branded goods and software.

In Australia it is estimated that nearly one-third of all software in use has been pirated. This has resulted in lost sales to the software, video game and toy industries alone of more than \$670 million a year. The internet has created a ready environment for the advertising

and distribution of counterfeit products on a global basis. Close to one fifth of Australian organisations who contributed to the PricewaterhouseCoopers *Economic Crime Survey 2007* believe that this situation is going to continue over the next couple of years.

Some of the most valuable assets an organisation possesses is its intellectual property and confidential information. Organisations should identify what confidential information they possess and determine the level of security to be applied based on its relative sensitivity.

It is important to think about access to photocopiers, and the ability to access electronic information with portable storage devices such as CDs, DVDs, flash-drives etc.

Case study:
Entertainment piracy

A major computer entertainment manufacturer believed that it was losing significant revenue to pirates and counterfeiters, who were distributing their product via classified advertisements, online and in suburban markets. The organisation estimated that it was losing 10% of its revenue in this way and that piracy accounted for 100% of units for its software in Australia (that is, for every legitimate computer game, there is a pirated one).

An anti-piracy investigation program was undertaken which included the use of undercover and surveillance operatives.

During the five-year campaign, more than 3,500 piracy cases were investigated, resulting in civil actions against organised pirates, and settlement awards to the manufacturer of over \$500,000. In some cases, matters were reported to law enforcement authorities, resulting in criminal prosecutions and convictions.

Case study:

Asian software piracy

A compact disk manufacturing plant in Asia was believed to be counterfeiting a large volume of an organisation's software products. A search warrant was executed on the suspect production facility and a forensic image taken of nine computers.

During the analysis an accountancy database was located on one of the computers. It was possible to establish the financial position of the counterfeiting manufacturer, and to obtain a full list of suppliers and customers. This database was successfully reconstructed and supplied in a working format to the client.

Keyword text searches were conducted on all computer hard drives discovered at the plant for supporting documentation. Numerous documents and spreadsheets were located, many of which were recovered from deleted areas of the drives. A number of the spreadsheets were password protected. These passwords were cracked using specialised software and found to contain relevant information.

A number of the documents located from text searches indicated a clear relationship between the factory and other organisations throughout Asia.

Information technology

Information technology is a significant part of the day-to-day operations for most organisations. But while the integration of technology results in many benefits, it also brings increased risks.

Information technology fraud can be defined as a criminal act in which a computer is essential to the perpetration of the crime. It can include hacking, mail-bombing, spamming, domain name hijacking, server takeovers, denial of service, internet money laundering, destruction or theft of data, electronic eavesdropping and unauthorised transfers of funds, electronic vandalism and terrorism, and sales and investment fraud. It can also include a criminal act where a computer, not essential to the perpetration of the crime, acts as a store of information concerning the crime.

Most information technology frauds are uncovered by accident or chance, revealing the inadequacy of many computer control systems to detect frauds. With increased dependence on information technology, the incidence of information technology fraud is increasing, and will continue to do so. This is explored further in Section 5.

Case study:

Leaked confidential information

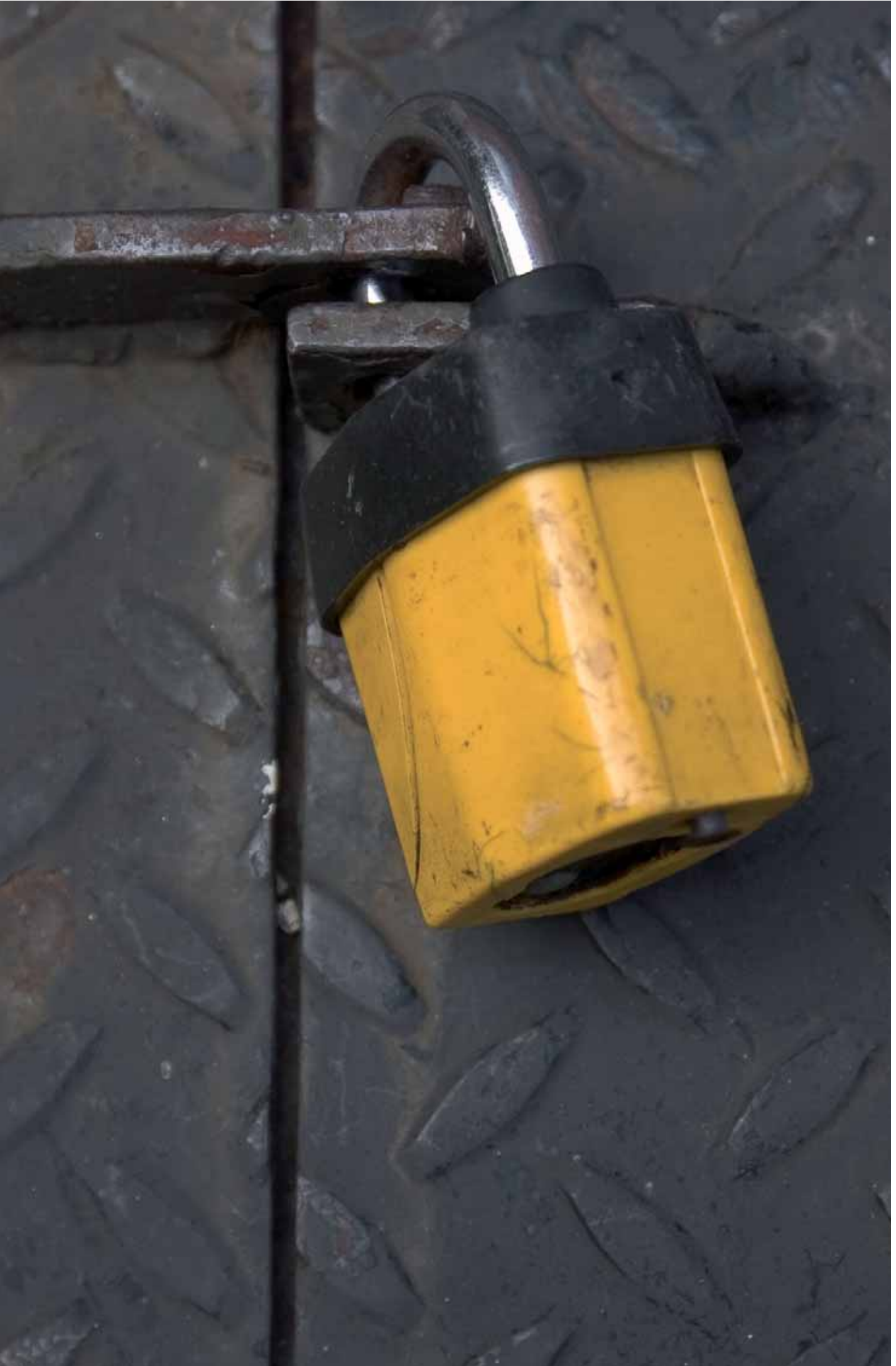
A group of employees in an organisation were suspected of leaking confidential information by electronic mail. It was alleged that this information was used by certain people to obtain financial advantage.

The computer network was logged to identify the movement of email attachments. Leaked documents were tracked exiting the organisation's network. Access was obtained to laptop computer systems used by employees and the computers were forensically imaged. Deleted electronic mail messages containing the document in question were recovered. A time line was constructed which identified the movement of the document through a chain of emails to outside parties.

Analysis of data and time information associated with the email messages and the attached document clearly identified the time period over which the leak had occurred. Analysis of hidden data within the document resulted in the identification of the original computer from which the document was first emailed, as well as the subsequent editing of the document by people in the electronic email chain.

The people responsible for editing and releasing the document were identified. Evidence collected was used in a successful civil action.





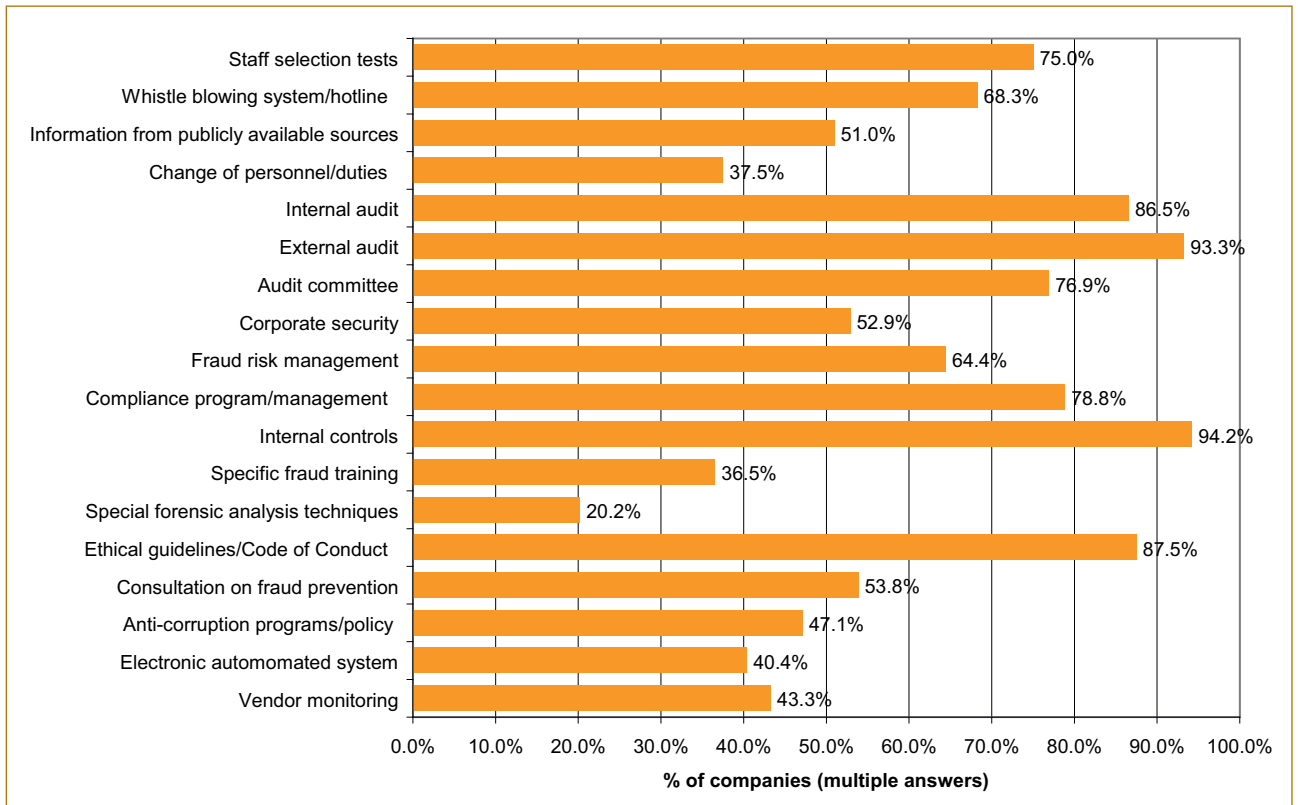
Fraud prevention techniques

Some easy-to-implement fraud prevention techniques

2

Markets are looking for a rigorous approach to risk management and loss prevention to safeguard business value. Increasing public awareness has also forced public institutions to take a more thorough approach to managing the taxpayer dollar.

Below are some basic fraud control and prevention techniques identified for Australian organisations from the PricewaterhouseCoopers *Economic Crime Survey 2007*. In combination with a thorough fraud risk assessment (as discussed in Section 1), detection methods and investigation plan (discussed in Sections 3 & 4), the use of these techniques should minimise the risk and impact of fraud in most organisations.



According to the survey, the vast majority of organisations in Australia and around the world have at least some specific fraud prevention measures in place.



There are four key elements to effective fraud prevention:

1. Oversight by the board and audit committee
2. Policies and training
3. Employment screening
4. Internal fraud controls.

Oversight by the board and audit committee

The board is responsible for overseeing the internal controls over financial reporting established by management and the process by which management satisfies itself that those controls are working effectively. The board is also responsible for assessing the risk of financial fraud by management and ensuring controls are in place to prevent, deter and detect fraud by management. Much of the board's oversight is embedded in the other elements of an effective anti-fraud program.

The organisation's board of directors and audit committee significantly influence the control environment and 'tone at the top'. They should therefore both be free from management's influence.

It is critical that the board and audit committee systematically and periodically review management's controls over financial reporting and other operations. It is also critical that such responsibilities for oversight be reflected in their respective charters.



Oversight should extend to:

Management

- anti-fraud programs and controls, including the identification of fraud risks and implementation of anti-fraud measures
- the potential for override of controls or other inappropriate influence over the financial reporting process
- review of accounting principles, policies and assumptions used in determining significant estimates
- review of significant non-routine transactions.

Employees

- mechanisms for reporting concerns.

Reporting

- receipt and review of periodic reports describing the nature, status and eventual disposition of alleged or suspected fraud and misconduct
- functional reporting by internal and external auditors to the board and audit committee.

Internal Audit and other bodies

- a plan that addresses fraud risk and a mechanism to ensure that Internal Audit can express any concerns about management's commitment to appropriate internal controls or to report suspicions or allegations of fraud
- involvement of other experts such as legal, accounting and other professional advisers as needed to investigate any alleged or suspected wrongdoing.

Scope of the directors' oversight

Appropriateness of the board and audit committee's oversight as it relates to fraud should be evidenced through discussions with members plus management and reported in the minutes. The scope of their oversight should include:

- considering the nature and frequency of their meetings and assessing whether adequate time is dedicated to considering fraud
- ensuring that audit committee members consider fraud in their review of:
 - accounting principles, policies and estimates used by management
 - significant non-routine transactions entered into by management
- evaluating management's assessment of fraud risk
- holding discussions with the external and internal auditors as to their views on the potential for fraud.

Policies and training

The development and implementation of a rigorous fraud control policy document for most organisations is a critical step toward effective fraud prevention.

Staff can only be expected to comply with policy if it is clearly set out in a comprehensive document which details procedures to be followed. Where no such document exists, it is often difficult to prove that employees or external parties have knowingly acted against the interests of the organisation.

Indeed the lack of clear guidelines is often the first excuse offenders will use when questioned concerning fraudulent acts.

A comprehensive policy

In conjunction with an effective code of conduct, a comprehensive fraud control policy document should be distributed to all employees, who should be asked to sign a declaration that they have read and understood the policy requirements.

The policy document should also set out other matters such as the responsibility for fraud control, employment screening, a fraud awareness program, risk assessment program, and the consequences of fraudulent action and/or withholding information concerning any such action.

Further, the organisation's policy should state clearly the intention to investigate suspicions and prosecute fraudulent acts. It should also explain the organisation's rights in relation to such things as access to workplace email and computer systems and the intention to recover any money or property lost as a result of such action.

Case study: Policy deficiencies

An external review of a state government agency's policy found that it had no responsibility structure, an inadequate definition of fraud, an inconsistent fraud reporting system and a lack of line management accountability. Subsequently the policy was re-drafted to take into account the latest developments with fraud control and the recommendations of AS 8001-2003. The agency now has a solid base upon which to progress its fraud prevention and control strategy.

Specific and general training

Employees should receive training at the time of hiring and periodically thereafter, addressing components of the policy such as:

- acceptance of gifts and entertaining
- conflicts of interest
- suspicion reporting/protected disclosures
- criminal and/or civil redress against offending persons
- breaching the policy guidelines
- investigation standards.

Organisations should also consider more general training in fraud and ethics awareness.

Case study: Fraud and ethics awareness training

A global telecommunications equipment manufacturer engaged advisers to develop and deliver a fraud and ethics awareness training package to every employee of the company in Australia and New Zealand. The company had previously detected inconsistent application of their code of conduct and anecdotal evidence suggesting awareness of fraud risk management and business ethics was deficient. Such deficiencies were addressed by open discussions on ethical 'grey' areas and related issues, organised as part of the training package.

Employment screening

The *PricewaterhouseCoopers Economic Crime Survey 2007* identified that approximately 71.4% of all fraud was committed by internal perpetrators.

Employment screening is therefore the first line of defence against fraud, and yet it is only in the last few years that many organisations have come to appreciate its importance. As a result, pre-employment screening has been included in the Australian standard on fraud and corruption control, AS 8001-2003.

This change of thinking is the result of circumstances such as publicity concerning organisations who have unwittingly employed criminals in high security or sensitive positions, and in many cases from personal experience involving candidates with false qualifications.

In recent years many cases have been publicised which adequately demonstrate that proper employee screening is not a luxury option. Disaster could have been averted if proper employment screening had been carried out. It is a fact that the cost of proper screening is far outweighed by the cost of one bad recruit.

To reduce exposure to avoidable fraudulent activity, an organisation should have clearly defined pre-employment standards which must be satisfied.

The candidate

The first source of information is the candidate. A comprehensive application form should be completed by all candidates. Candidates should be advised that it is the organisation's policy to carry out in-depth screening prior to their appointment, and should ask candidates to sign a release form or similar document.

Detailed checks

The application form and the CV provide the basis for detailed checks to be carried out with referees, educational institutions, previous employers and public records. The following should be undertaken as a matter of course:

Reference checks

- referees and previous employers (preferably line managers) should be spoken to after their identities are independently confirmed
- bear in mind that referees provided by the candidate are unlikely to provide unfavourable information even if they are aware of such information.

Qualifications

- all educational certificates should be inspected and independently verified
- be aware that desktop publishing enables convincing documentation to be produced with little effort
- contact the institutions for verification of qualifications and professional memberships, rather than relying exclusively on candidate-supplied certificates.

Background searches

- Background searches should be undertaken using public databases and information sources. These might include directorship searches to ensure there are no potential conflicts of interest, bankruptcy searches, and media searches.
- Criminal record searches might also be considered.

Taken together, the above checks should help build an accurate picture of the candidate's experience, background and qualifications.

A specialist task

Effective employment screening is a specialist task requiring investigative skills and access to a wide array of public information databases. Many organisations, particularly those involved in financial services, prefer to outsource this work to screening experts. Further, it should be remembered that very few placement organisations perform employment checks to the standard recommended in this guide.





Internal fraud controls

There are many different ways that organisations can protect themselves against fraud in the common risk areas that were identified in Section 1. Some of the more effective controls in common areas of business are as follows:

1. Purchasing and payroll

The following are some ways in which organisations can protect themselves against fraud in purchasing and payroll:

- keep copies of invitations to tender on file for future inspection, to ensure that specifications are identical (i.e. no organisation is given a more difficult specification to cause them not to bid or to submit a higher bid than it otherwise would)
- require contracts to carry a 'right to audit' clause to facilitate an audit of the supplier's records should evidence of corruption come to light
- ensure suppliers and staff are fully aware of the organisation's policies on code of conduct, gifts and entertaining, and conflicts of interest
- ensure demand levels are clearly understood to avoid unnecessary over-ordering
- establish clear purchasing authorisation levels, and monitor these to ensure they are reasonable
- pre-qualify of prospective suppliers ('due diligence')
- ensure there is appropriate segregation of duties between the maintenance of supplier master file data, purchasing, authorisation

of purchases, invoice processing, the payment of invoices, accounting and bank reconciliation processes

- apply strict controls to supplier and employee master file data, including procedures to monitor dormant suppliers and employees to prevent illicit alterations
- conduct regular checks of employees to verify their existence
- conduct regular checks of overtime payments.

It is also good practice to carry out periodic checks to ensure that invoices are from genuine organisations, and not from shelf organisations operating from 'serviced office' addresses or false invoices printed to facilitate payment against non-existent suppliers of goods or services. Automated detection testing programs can be used for such checks. Section 3 contains further details.

Case study: Purchasing fraud

A large manufacturing organisation had received numerous anonymous complaints about a particular employee over several years. Background enquiries revealed that the employee was connected to several organisations based in the local area. Forensic examination of the suspect's work computer located financial records of these organisations, which indicated they had been trading extensively with a major supplier of the organisation.

Forensic accounting examination of these records revealed that the services allegedly provided by the supplier had in fact been provided by the employee's organisation. The supplier had been merely acting as a 'middleman'. The services supplied were grossly overcharged and in many cases no service had been supplied at all. Approximately \$2 million of losses were suffered under this scheme.

2. Sales and inventory

Practices recommended to prevent fraud in sales, inventory and debtors include:

- ensure appropriate segregation of duties are in place between sales, assignment of credit notes, accounting, inventory and bank reconciliation processes
- warehouses should always be maintained under strict security and surveillance; no inventory should be permitted to leave a warehouse without appropriate checks that the inventory ordered matches the inventory being removed
- cash registers should also be maintained under strict physical security and surveillance to identify instances of unrecorded sales by sales staff
- voided, cancelled or 'no-sales' cash register entries should be documented and authorised by a non-sales staff member. Auditing programs should also be used to monitor these instances.
- discounts should be monitored regularly using auditing programs, and discount levels should be set and maintained by non-sales management

- credit notes and the issue of credit on account should only be awarded following authorisation by non-sales staff
- outstanding debtors balances should be closely monitored, especially in cases where employee sales commissions are paid – debtors themselves should be verified and outstanding debtor balances checked as being legitimate sales and debtor transactions
- automated detection testing programs can also be used for undertaking periodic checks for fraudulent transactions
- careful attention should be paid to debtor queries around outstanding balances to ensure that debtor balances are correct and that debtor payments have not been misappropriated.

Extra care with sales and inventory controls would appear to be common sense, yet many frauds occur in this area because controls are ignored or not enforced. This is particularly the case in organisations with a strong 'sales at any cost' culture.

3. Cash and cheques

Theft of cash and cheques remains a major problem for many Australian organisations despite EFT systems being in common use. Recommended controls include:

- Conducting regular – even daily – bank reconciliations by someone independent of the cheque and EFT payment process
- Reviewing all cheques made out to cash and avoiding the use of manual cheques
- Following up complaints from suppliers or customers concerning outstanding balances.

Case study: Sales commission fraud

A publishing organisation was concerned about the high outstanding debtor balances in the accounts of a remote subsidiary. Enquiries made to some of the debtors identified a number of suspect sales transactions which were denied by the debtors.

Investigations revealed that a particular sales manager with access to sales records had created fraudulent sales using existing debtor accounts, in order to generate fraudulent commissions. Although the total amount of the fraudulent commissions was small, the corresponding revenue overstatement amounted to \$800,000.

Evidence included statements from the debtors and audit logs showing the creation of the sales on the system by the sales manager. Further enquiries revealed the suspect had also processed a number of fraudulent accounts payable cheques.





Proactive fraud detection

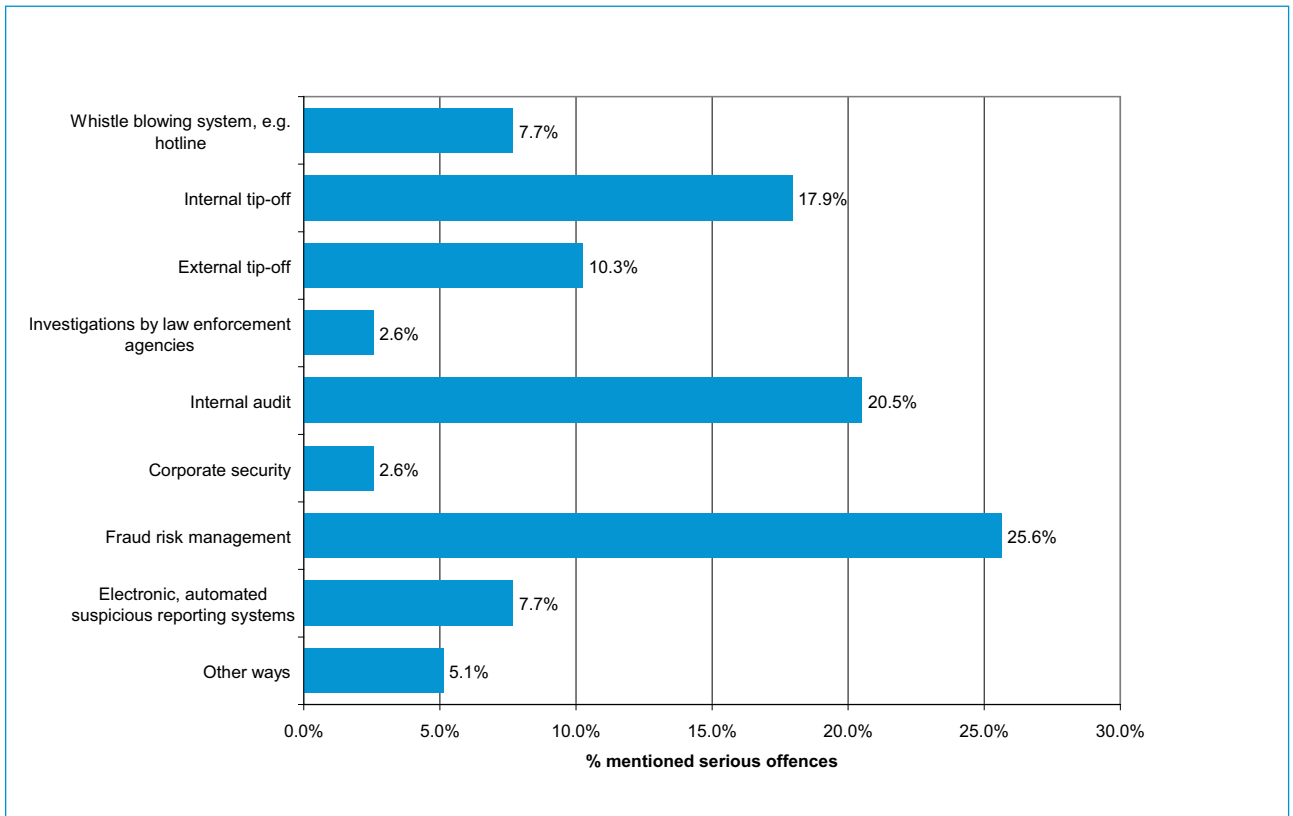
Making fraud detection part of business-as-usual

3

Proactive fraud detection is based on a simple fact: the vast majority of successful cases occur as a result of apparent accident or tip-off.

The PricewaterhouseCoopers *Economic Crime Survey 2007* for Australia found that in most cases frauds were not detected by specific preventative or detective measures, but rather were revealed through external or independent business functions.

The following diagram from the PwC survey tells the story:



Based on these statistics, which align with anecdotal experience, the key to successful fraud detection is facilitating tip-offs through whistleblower programs, and by putting in place detection programs such as suspicious transaction analysis, that replicates the ‘accidental’ discovery.

Through a whistleblower protection program and other investigative services an organisation clearly demonstrates its commitment to good corporate governance, comprehensive risk mitigation and the establishment of an organisational culture that promotes a high degree of ethics

and belief in its stated corporate values.

Protected disclosures/ whistleblower protection

A fraud control policy should make it clear that it is the responsibility of staff to report any malpractice to management. In practice there is often a reluctance to do this as some staff interpret it as ‘dobbing’.

Because of this, the development of a protected disclosures (whistleblower) program is an important element of any effective fraud prevention or mitigation strategy.

An example is fraud ‘hotlines’, which are proving useful as a means of encouraging the reporting of fraud incidents, either anonymously or otherwise.



Such a program should be designed to:

- encourage the reporting of incidents of fraud, corruption, legal or regulatory non-compliance, and questionable accounting or auditing matters
- allow for the efficient and effective investigation of disclosures
- protect those making the disclosure from reprisal
- appropriately manage those subject to an allegation.

In their 2006 *Report to the Nation on Occupational Fraud and Abuse*, the Certified Fraud Examiners established that 44% of million dollar frauds in the US were discovered as a result of tip-offs. Similar results were found by the PricewaterhouseCoopers *Economic Crime Survey 2007* for Australia (see *whistle blowing system in the diagram on page 22*).

Legislators in the US have moved to compel certain organisations to protect genuine whistleblowers through provisions in the Sarbanes-Oxley Act of 2002.

In Australia, CLERP 9, AS 8004-2003: *Whistleblower Protection Programs for Entities*, ASA 240 and the Australian Stock Exchange Corporate Governance Council's *Corporate Governance Principles and Recommendations* have placed an impetus on organisations to establish an effective whistleblower system. In many cases, state based government organisations have legislated whistleblower obligations. The Corporations Act also places certain obligations on companies receiving disclosures, touching up on breaches of corporations legislation.

How to implement a protected disclosures program

There are four essential components to an effective whistleblower protection program, as follows:

Develop a whistleblower protection policy and procedures

A policy should be developed that:

- complements and enhances the already established communication channels between employees and supervisors
- protects employees from reprisals that might otherwise be inflicted as a result of their disclosures
- ensures disclosures are properly investigated and dealt with
- ensures relevant disclosures are appropriately reported to senior management.

Develop a disclosures database

A secure database should be built to record details of disclosures, including details of progress of investigations and the ultimate disposition of matters. It is important that access to this database be strictly limited.

Implement methods of receiving disclosures

There are a number of ways to receive disclosures, including telephone, ordinary mail, email and facsimile. In our experience, setting up a single free-call telephone number is the most effective method of receiving disclosures. In this way the investigator can immediately commence to build rapport with the caller at the time of the initial call and there is a greater chance of obtaining all relevant information.

We recommend the line be open between at least 8.00 am and 8.00 pm so calls can be made

before or after normal work hours.

Communicate and train

The key to any successful disclosure hotline is an effective awareness and communication program. An important aspect of this training is fraud prevention and ethics awareness as well as detailed training on organisational policies and procedures to prevent misconduct. Options for delivering training include:

- conducting workshops for all staff
- conducting 'train the trainer' workshops
- online training rolled out over the intranet/internet
- a combination of all of these.

Appropriate promotional material, including posters, brochures and tactile cards should be developed, and appropriate material should also be accessible on your intranet. In all these materials a statement assuring staff of confidentiality should be prominently displayed.

Case study:

Whistleblower protection policy and set-up of an external hotline

A publicly listed company in Victoria required a whistleblower protection policy and an externally managed hotline that could receive disclosures from staff and the general public.

With the aid of external advice, the company developed a whistleblower protection policy, including a 1800 telephone number, PO Box, and a database accessible on the organisation's website for the receipt of disclosures. Experienced investigators manage the system, reporting disclosures to the organisation's whistleblower protection coordinator with recommendations for further action.

Acceptance of the hotline

Feedback to those who use the whistleblower service is critical to its perception within the organisation.

When assisting callers, investigators attempt to establish rapport and trust. Each caller will be given a unique identification number. Although some callers may wish to remain anonymous, all callers should be encouraged to identify themselves. If the caller wishes to remain anonymous, their identification number can be used. They should be asked to call back within a week so the investigator can provide feedback and perhaps seek further information.

If the caller was identified, the investigator will arrange an appropriate time to provide feedback and perhaps seek further information.

'Suspicious transaction analysis' – Automated detection programs

It is possible to discover indicators of fraud within an organisation's financial records, even where there is no prior suspicion. Usually, such indicators are obscured within the millions of items of valid data held in those records. Manual testing is rarely an effective or efficient solution, and hardly the job of time-pressed management or external auditors.

An automated fraud detection methodology can search through millions of transactions and other data quickly to identify anomalous transactions which might be worth a closer look or further investigation. This is particularly true of purchasing, payment and expense records which are high risk areas in many organisations, although automated testing can also yield results in sales, inventory, insurance claims, superannuation payments and entitlements and other areas of business.

Some of the more useful tests are as follows:

Employee and payroll tests

- payroll payments with no tax deducted
- employees receiving excessive overtime as a proportion of total salary
- payroll payments to employees prior to hire date or after termination date
- unusual dates of birth.

Purchasing and payment tests

- split purchasing to avoid purchasing limits
- payments to suppliers where the bank account matches an employee bank account and the supplier name differs from the employee name in the event employee related suppliers reside on the supplier master file

- duplicate supplier payment transactions with the same amount and either the same or similar invoice number.

Customers and sales tests

- excessive refunds, credit notes or discounts issued to customers
- refunds, discounts or credit notes to customers where the customer address or name matches an employee's address or name
- collusion between employees and customers.

Automated fraud detection is a form of data mining and as such it is evolving with technology. Testing which effectively risk-scores every transaction according to 'hits' in particular tests is the latest development. In theory, it is possible to identify the single most risky transaction among millions – literally finding the 'needle in the haystack'.



Case study:

Fraudulent collusion between suppliers and employees

Analysis of payments carried out for a large insurance organisation identified duplicate claim payments and suspicious payments to suppliers sharing an address with an employee.

The payments were proved to be fraudulent and were reported to the police. This led to criminal charges being laid.

Case study:

Duplicate payment of supplier invoices and cleaning of supplier master files

External analysts contracted by an organisation identified \$600,000 of duplicate invoice payments over a two-year period. An automated detection program established that these had occurred because a number of suppliers had been entered on the supplier master file more than once, allowing for the easy processing of duplicate invoices.



Case study:

Overpaid overtime

External analysts were contracted by a government agency to analyse staff salaries and overtime payments over a three year period.

The analysts identified nine employees who were paid overtime rates in excess of \$1000 per hour, the highest being \$4,989 per hour. These results allowed the agency to investigate the payments and recover the over-payments.

The value-add of data mining

An automated fraud detection program can provide management or the auditor with, for example, a detailed list of questionable transactions, employees and suppliers which need further investigation.

In larger organisations, automated fraud detection tests conducted before an audit will also complement an organisation's schedule of audit visits, making

the best use of valuable and often scarce resources. It is a tool which will quickly identify problem areas and can also be used to audit the records of suppliers where a 'right to audit' exists. The process is simple and time-efficient and is not disruptive to normal business operations.

Automated fraud detection has been found to be particularly beneficial when conducted annually. Annual analysis not only allows an

organisation to regularly identify transactions of interest, it also allows them to determine whether control or process changes, made as a result of a previous analysis, have resulted in a decreased number of transactions of interest in the subsequent year's analysis.



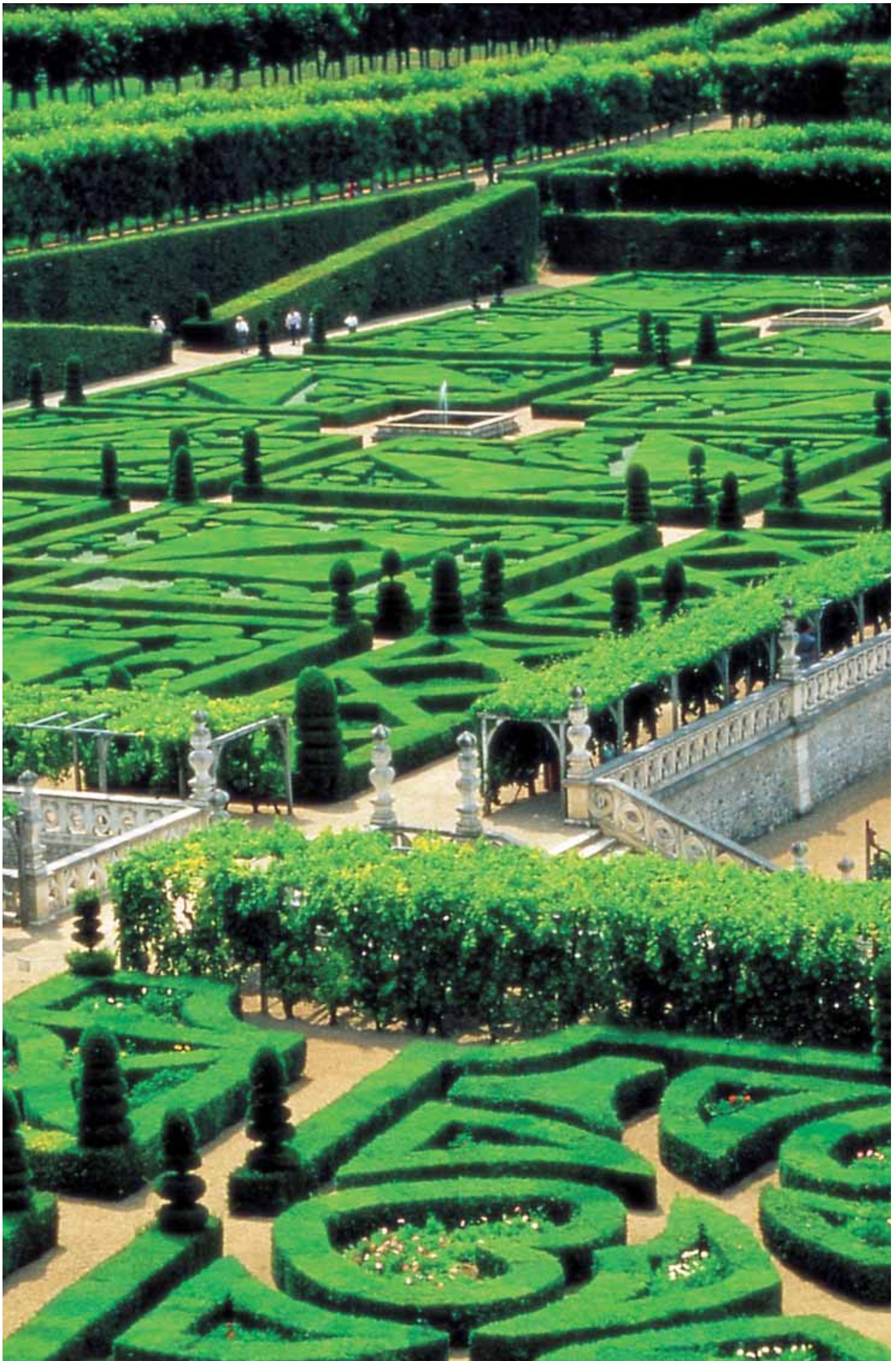
Case study:

Vehicle over-servicing

Unsatisfied with the operating costs of its vehicle fleet, particularly relating to vehicle maintenance, the organisation approached external analysts to undertake a data review specifically over vehicle maintenance payments.

An analysis of all electronic maintenance data for the entire vehicle fleet over a three year period was undertaken. Several anomalies were detected, including apparent over-servicing of vehicles and vehicles serviced with either no labour costs or no parts costs. The fleet provider was able to revisit the service provider agreements with the intention of terminating the relationship with the vehicle maintenance provider.





Effective fraud investigation

A step-by-step plan

4



Fraud investigations are not like standard police-type investigations into criminal activity. This is because the majority of fraud investigations begin only with a mere suspicion that a fraud has occurred. In many cases, there is little initial evidence of that fraud, as the nature of most fraud is such that deception is involved in committing and then covering up the crime.

However, it is also true that most frauds leave a trail, or a series of indicators which suggest a fraud has occurred. The key is to locate those indicators as early as possible in the investigation.

Fraud investigation resources generally fall into four categories or skill-sets. In the majority of cases, most if not all of them are required to fully investigate a suspected fraud. These skill sets are illustrated and described below:



Investigation resources

Investigative intelligence and analysis

This is the research component of the investigation. It involves experts in publicly sourced information obtaining relevant information concerning individuals and entities suspected of involvement in the fraud. This is one of the first steps taken in an investigation where a suspect has been identified. Investigative researchers will quickly identify, for example:

- directorships and shareholdings in private companies in Australia and overseas
- mentions in the global media
- bankruptcy and disqualifications by regulators
- court judgments
- asset holdings.



Forensic accounting/transaction analysis

Forensic accountants are a vital piece of the investigation puzzle, as they are responsible for quantifying and evidencing identified fraudulent transactions. This can be a challenge in situations where the suspects themselves are skilled accountants and have knowledge of the financial system. Often, a forensic accountant will need to piece together incomplete or deliberately falsified financial records. Section 6 has further details about this.

Forensic accountants may also be required to calculate losses and damages and prepare insurance claims. You can read more about this on pages 32 and 33 under 'Fidelity insurance'.

Computer forensics

Computer forensics involves the search, seizure and analysis of electronic evidence, which is most often found on personal computers but can also be found on virtually any modern electronic device.

It is rare for modern day frauds to be perpetrated without the involvement of computers, and therefore computer forensics is a vital skill-set in the vast majority of fraud investigations. Section 5 has further details about this.

Fieldwork and interviews

Again a crucial part of most investigations, interviews with witnesses and suspects can prove vital to an investigation. Statements made during an interview can become admissible evidence, if obtained in an appropriate manner.

Responding to a fraud incident

The following plan is a guide to the actions that should be taken in the event that a fraud incident occurs, or suspicion of a fraud arises. Of course, every fraud incident is different, and reactive responses will vary depending on the facts that are unique to each case. However, this plan is a typical response which can be used as the basis for responding to any fraud incident.

Before you start

When fraud is first suspected, the matter could be more serious than it may initially appear. This is because financial criminals rarely restrict their activities to only one *modus operandi*. Therefore every effort should be made to obtain as much information as possible before anyone is questioned, confronted or interviewed. This is particularly important in organisations or business units with a close working environment, where there may be a strong temptation to simply question an employee as soon as a suspicion is raised.

It is also important to be aware that larger scale frauds of the modern era are often international in nature. Therefore, any fraud contingency planning must include measures for taking legal and investigative action across jurisdictions.

Initial actions are crucial to the eventual outcome of an investigation and, if a proper strategy is put in place and adhered to, the extent of fraudulent activity can usually be assessed and action taken to resolve the matter successfully.

Assign responsibility

Fraud investigation is by necessity a confidential task and is a sensitive matter for the vast majority of organisations. It is vital that all allegations of fraud are treated seriously and that responsibility for handling fraud incidents is assigned to a senior, trusted individual or collection of individuals.

In many organisations, responsibility is handed to a corporate security advisor, internal audit or risk management director or manager. In other organisations, the responsibility is shared between members of senior management or an audit committee, and the organisation's human resources personnel and corporate lawyers are involved from a very early point. Fraud incident management responsibility is an important role, and those chosen to administer the role must come from the appropriate legal and management level to authorise investigative actions and to co-ordinate the organisation's overall response to fraud incidents.

As part of its overall fraud control plan, organisations should assign responsibility for fraud incident management to an appropriate person(s) as a precursor to adopting an incident management plan. Consideration should also be given to the appropriate level of involvement by corporate lawyers and human resource personnel.

Case study:**Telecommunications dealer fraud**

A large telecommunications dealer outsourced its customer acquisition process to a national retail store. Over a nine month period an organised crime group targeted the retailer using fabricated proof of ID to support applications for phone service and handsets. As a result the telecommunications dealer lost 200 handsets valued in excess of \$100,000. Commissions due to the retail store amounted to a further \$80,000.

It was suspected that “backhanders” were being paid to vulnerable employees. Analysis of the customer application forms confirmed the systematic use of false IDs together with the involvement of one particular employee. By producing a timeline of application frauds and matching this with employee time sheets and signed telephone contracts, it was possible to positively identify one perpetrator. Evidence gathered included; customer application forms, photocopied proofs of ID, telephone billing records and statements from genuine customers whose ID had been misused.

The employee was interviewed, resulting in summary dismissal. It was subsequently discovered that the gang had committed similar offences at other retail stores nearby. As a result, the case was passed to local Police, dealer commissions of \$80,000 were withheld, and new processes to control organised application fraud were recommended and introduced by the telecommunications dealer.

Receipt and initial assessment of suspicion, allegation or ‘tip-off’

As discussed previously in Section 3 of this guide, fraud investigations are often initiated after an allegation or tip-off (often anonymous) is received by someone in the organisation. This will usually be sourced from inside the organisation, although external tip-offs are not uncommon. Many fraud incidents are initially discovered by accident, perhaps as a result of an audit, job change, or

resignation. Very few frauds are discovered as part of a deliberate attempt to uncover fraud, as very few organisations implement a proactive fraud detection program.

The following actions should be taken in all cases where a fraud suspicion or complaint is received:

- alert the fraud incident manager that an allegation or suspicion exists
- obtain as much detail about the allegation as possible. This detail should include the name of the ‘informant’ and full details concerning the alleged fraud. A written statement from an informant may prove to be vital evidence if legal action is contemplated at a later stage. If possible, an interview should be arranged with the informant.
- at no time should the suspect be alerted that an allegation has been made
- list all circumstances surrounding the allegation or suspicion
- maintain a log of all actions taken since the information was received
- prepare accurate file notes of any conversations or correspondence which has occurred. These become contemporaneous notes that may be required for court proceedings at a later stage
- only advise/involve those who *absolutely* need to know.

At the conclusion of this stage, a decision must be made as to whether the allegation or suspicion warrants investigation, or is implausible or vexatious. However, this decision must be made carefully. If an allegation

cannot be quickly dismissed as false, further action should be taken as follows.

Initial investigation

Once a fraud allegation is received and a fraud incident manager is alerted, an investigation plan or strategy must be devised which will prove, or disprove, the allegation. This strategy will be dependent upon a number of circumstances, such as:

- whether the suspect(s) are aware of the allegation or suspicion
- whether the suspect(s) are employees
- whether the suspect(s) work in the premises
- whether the alleged fraudulent activity is ongoing
- the intentions of management should the allegation be proved.

Many organisations choose to involve their legal advisors at this point, and involve those advisors in devising the investigation strategy. While lawyers are not investigators and should not be considered such, their input will be required in relation to legal options and employment-related matters.

(a) If the suspect is a current employee

When devising an investigation strategy, the following information and evidence gathering techniques should be considered:

- full background searches of suspect companies and individuals using public databases and information sources

- Out of hours search of a suspect's desk/office/work area for incriminating evidence in files, notes, diaries and other work related sources. An exhibit log should be utilised during this search to record the details of any evidence located. These details will include who found the item, when it was found, where it was found, and a full description of the item. **It is strongly recommended that specialist advice is sought prior to a search to ensure compliance with relevant law.**
- Imaging and analysis of the content of a suspect's office personal computer (and possibly any relevant file servers), using specialist software (such as EnCase) to recover deleted or hidden files can often reveal documents of interest. It is essential that only trained computer forensic experts are used to conduct this part of the investigation. Utilising in-house information technology staff can lead to information being lost and evidence being declared inadmissible in court, due to the methodology used (refer to Section 5 of this guide for more detailed information on computer forensics). Forensic imaging of computer systems may be covered by legislation such as the Workplace Surveillance Act in NSW (Refer to Section 5 page 36) where an organisation's policy must alert employees to the organisations' right to image and analyse those systems.
- Analysis of calls made from office telephone and facsimile lines of a suspect to identify non-business related calls (e.g. calls to offshore banks, real estate agents and so on). In certain circumstances

employee telephone calls are routinely recorded and if so such recordings should be secured and reviewed for relevance.

- 'Forensic accounting' – detailed review and analysis of transactions, documents and files
- and where necessary:
- surveillance of suspect to identify associates, evaluate lifestyle, and other sources of income
 - forensic examination of documents including handwriting analysis and 'Electro Static Detection Apparatus' (ESDA) testing.

The above actions should not be conducted if they constitute a risk of alerting the suspect to the investigation.

(b) If the suspect(s) is a third party, supplier, customer, etc.

There are limitations on the information which you may legitimately gather concerning the actions of a third party. However, the following techniques may prove useful:

- detailed background searches using public databases to determine company directorships, shareholdings, media reports, and corporate credit reports statements from staff concerning the activities of the third party
- statements or other information from other third parties with knowledge of the suspect or the suspect(s) activities
- detailed forensic examination of documentation concerning all transactions, correspondence and interaction with the suspect third party

- surveillance of suspect to identify associates, evaluate lifestyle, and other sources of income
- document forensics including handwriting analysis and ESDA testing.

It should be noted that many of the techniques listed above are specialist tasks, and that many require specialised equipment and technology. Serious consideration should be given to outsourcing these investigations to external experts, if such expertise cannot be found internally.

External investigations should not be considered in isolation, as most external frauds have an element of internal collusion involved. The possibility that personnel may have colluded with third parties to defraud the company should be considered when undertaking investigations.

Case study: Banking fraud and asset tracing

A web of suspicious financial transactions through an Indonesian bank was investigated. This assignment involved complex asset tracing and enquiries into the involvement of senior government officials and members of the Indonesian banking community.

Work was conducted under the fierce glare of publicity, in a highly politicised environment where the emphasis was on the maintenance of absolute independence and integrity. The report was presented to the Indonesian parliament, and various charges were laid against individuals involved in the matter.

Suspect interviews

Many investigations conclude with a formal interview with the suspect(s), during which all evidence will be put to the suspect under controlled conditions. Suspect interviews should only be undertaken by skilled, experienced investigators. In most cases, they should only be conducted once all investigations are complete.

There are rules concerning the conduct of interviews and legal requirements for statements, although these are beyond the scope of this guide. Legal advice should be sought before interviews are conducted unless using trained, specialist investigators.

Reporting of investigation findings and subsequent actions

Armed with evidence gathered from the investigations undertaken, the incident controller(s) should obtain legal advice as to the appropriate way forward. This counsel should be considered together with the organisation's overall objectives and policies. Typical conclusions and options at this point could include:

- **the evidence is insufficient or inconclusive:** no further action
- **the evidence is strong, but requires further support:** continue investigations and consider legal action for Anton Pillar Orders/Mareva Injunctions (See 'Legal actions' detailed on this page)
- **the evidence is conclusive:** take disciplinary action against suspect employees; consider legal action for civil recovery from guilty parties; and consider referring the evidence to the police for investigation.

Legal actions

Likely legal actions against suspects in fraud matters include the following:

- Mareva injunctions against the suspect (this has the effect of freezing assets and causing the suspect to disclose to the court all assets wherever they may be)
- Anton Pillar relief (this is a court order which permits lawyers for the aggrieved party to search the premises of the other side for specified documents), and other court orders which lawyers can rely upon in civil actions against the fraud suspect
- civil action for recovery of defrauded funds, losses, and damages.

Alternatively, you may prefer (or be required) to alert the police who will consider your claims and evidence before deciding whether to pursue the matter in the criminal arena.

Police referral

Referral of fraud incidents to the police is a preferred course of action, and is a legal obligation in some jurisdictions. However, it must be understood that police action in fraud matters will usually only proceed once the police have received a detailed incident brief of evidence which sets out the allegedly fraudulent activities, and provides sufficient evidence to support the allegations.

Major fraud incidents are usually referred to specialised 'fraud squads' such as the NSW Commercial Crime Agency. However, local police stations also investigate and prosecute fraud offences. The fraud squads are specialist task forces which tend to investigate frauds of

a large, complex, protracted, political or cross-jurisdictional nature. In many cases, referrals of smaller value or 'simple' fraud offences may be better directed towards the local police station.

Most fraud referrals are required to be 'assessed' by a police assessment committee, as suitable for police investigation and prosecution. Successful assessment depends very much on the nature and seriousness of the offences, and the quality of the supporting brief of evidence.

Fidelity insurance

Fidelity insurance is infrequently used in Australia. When a fraud incident occurs, it is often a valuable recovery option. However, organisations must be aware of their requirements to make a claim under their fidelity insurance policy. These requirements might include:

- immediate notification that an incident has occurred
- reporting of the matter to police
- an independent investigation and production of evidence
- quantification of losses.

A joint study by PricewaterhouseCoopers and the Australian Institute of Criminology – *Serious Fraud in Australia and New Zealand (2003)* revealed that victims of fraud recovered, on average, only 10% of the loss incurred following a criminal conviction of an offender. This is further substantiated by the PricewaterhouseCoopers *Economic Crime Survey 2007* results for Australia.

This survey highlighted that although 63.7% of respondents in Australia have insurance to cover loss as a result of economic crime (fraud), 81.1% of respondents

were unable to recover any losses through insurance. Furthermore, only 8.1% of organisations have been able to recover more than 60% of their losses through insurance.

Fraud and theft related insurance coverage should be evaluated and reviewed according to relevant risks. Fidelity insurance is notoriously difficult to claim against, yet it may be the only means of recovering funds lost through fraud.

Personnel management

An important and often neglected aspect of fraud incident planning involves the internal and external management of the incident after the investigation has been completed and legal or police action has been initiated.

In most cases, police involvement in a fraud incident will bring the matter into the open, as far as the affected organisations are concerned. Rather than avoiding comment on the matter, or relying on office rumour, it is far better to officially notify staff that an investigation into alleged fraud has been conducted.

Internal announcements

Internal announcements covering fraud incidents should stress that:

- management takes these matters seriously, and that corporate policy dictates that all such matters are prosecuted
- the matter has been reported to the police
- any approach for comment from external sources such as the press must be directed to a designated representative. Staff should make no comment whatsoever to external parties.

Public announcements

Most organisations choose not to precipitate an announcement to the press or public unless that becomes necessary, however it is useful to have a prepared plan should the matter become public knowledge through the press or court announcements. Such a plan should be prepared in consultation with public relations and media advisors, as well as legal counsel.

In preparing a response to any press report, consideration should be given to the following points, along the lines of the internal announcement, in particular:

- stressing that an incident has been investigated, and that the matter has been reported to the police who are investigating
- stating management's policy to pursue any and all such matters rigorously through the courts.

Specific references to suspect names, dates, amounts, etc. should usually be avoided. The purpose of the public announcement should be to affirm that management is fully aware and in control of the situation, and also to affirm the organisation is in no way a 'soft target' in these matters.

Follow-up reviews

Once a fraud incident has been investigated and actions have been taken, there is often a temptation to assume that the matter was isolated and could never happen again. A follow up review should be undertaken which achieves the following:

- identifies, reviews and strengthens controls which may have failed, or which were bypassed or overridden in committing the fraud

- develops or refines the fraud incident plan to make it more effective
- implements proactive fraud detection mechanisms designed around the *modus operandi* used to commit the fraud, to increase the likelihood of detecting similar frauds in the future.

Case study: Employee fraud

Anonymous letters were sent to two government agencies alleging that a government employee was involved in fraudulent activity. The suspect was a senior manager with control over finance, payroll, human resources and training operations.

Steps were taken to ensure the suspect employee was suspended during the investigation. Initial investigations involved the recovery of deleted computer records and interviews with staff members who provided numerous leads. A wealth of information was uncovered, including evidence the suspect had:

- falsely obtained employment with bogus qualifications and a false employment history
- a prior conviction
- forged documents and falsified accounts
- misused stolen employer assets
- committed credit card application and expenses fraud
- evaded income tax and conspired to defraud public revenue (FBT fraud)
- collected unauthorised increases in salary and bonuses
- been absent from duty and made claims for work not performed
- colluded with a contractor to pay for services not performed.

A criminal brief of evidence was prepared for the police and evidence given at the trial of the offender. Assistance was provided to the organisation's legal advisers in handling the offender's dismissal, resulting in a defeated 'unfair dismissal' claim. The offender was convicted and sentenced to prison.



Electronic investigations

What if there's no paper trail?

5

Traditionally the collection of evidence in a fraud investigation has relied upon the presence of a physical paper trail.

In today's corporate environment, the paper trail largely originates from, and in many cases has been replaced by, records from personal computers and other electronic devices such as PDAs. In response to this trend, a field known as 'computer forensics' has developed. Computer forensics is the seizure and analysis of electronic data using a methodology which ensures its admissibility as evidence in a court of law.

Computer forensics is an integral part of modern fraud investigation.

Legislation in NSW has the potential to have an impact on an organisation's ability to investigate computer systems and electronic records such as email. From 7 October 2005, all NSW businesses are required to notify employees that electronic surveillance can be performed by their employer. If the employees are not notified and surveillance is conducted, it

is a breach of legislation and any evidence gathered is likely to be inadmissible.

The forensic image process

The fundamental principle of computer forensics is that original data is *never* altered. For this reason, purpose-written 'forensic image' software is used to take an exact copy of a 'target' computer system. From this image the original system can be recreated at any time. It is essential that trained and experienced specialists be assigned to this task.

This ensures both the integrity of the target system (it is difficult to put a monetary value on the accidental loss of commercial information), and the integrity of seized evidence. Computer forensic technicians or any one else who gathers computer-based or electronic evidence must be able to justify their actions in future court proceedings. We strongly recommend the use of

a computer forensics expert for advice rather than relying solely on an organisation's information technology staff.

Forensic computer images have been accepted by Australian courts. It is no longer necessary (in most cases) to seize physical computer hardware. Indeed, in situations where target computer systems contain critical data, such as in a doctor's surgery, physical seizure may not be a viable option. Once an image has been taken, hardware that may otherwise have been required to be secured for evidence continuity may be put back into use.

Forensic imaging is also well suited to covert investigations. Much information can be drawn from a suspect's personal computer without alerting him/her to an investigation.

Case study:

A law enforcement agency

A suspect was under investigation by police for a serious offence. The suspect based his innocence on an alibi stating that he could not have been present at the scene of the crime as he was at work using his computer to surf the internet when the crime took place. The validity of this alibi was questioned. Computers were forensically imaged and examined. Five sources of information were used to identify user activity. These included file data and time properties, program log files, email data files, internet usage, and text files containing relevant dates.

Analysis of times and dates in email headers on the computer and the server failed to show any activity for the specific times. Examination of temporary internet files revealed that none had been created with the relevant time stamps. A low-level text search was conducted across the entire contents of all the computer hard drives to locate any reference to

these critical dates. No records or test references could be found on any areas of the hard drive to support use of the computer for the times in question. In conclusion, the analysis strongly indicated that the computer was not used during the critical period. This was corroborated by records from the suspect's Internet Service Provider (ISP).

The individual was convicted at trial of the criminal offence. The electronic evidence was a key factor in the proceedings.



Data analysis

In the analysis phase, computer forensics is concerned with more than existing files. A computer forensic technician will examine the entire structure of a hard disk, looking to collect all possible evidence. During normal PC operation, data additional to that which the user intends to save is 'written' to the surface of the hard disk.

On examination such information can be located as:

File slack

Part of a space reserved for use by a file that has not been completely filled by that file. This information consists of data pulled from the computer's memory, used to 'pad' the file to the required length. Slack often consists of garbage text,

but on many occasions has been found to contain text relevant to the investigation.

Data fragments

Units of disk space that are in use but not accounted for by files on the disk. These fragments usually represent material left on the disk by old files or applications.

System slack

Data written to areas of the hard drive reserved for use by the computer's operating system. Some programs use this area as temporary storage. On many occasions valuable evidence from these areas has been collected from computer systems which were previously believed to be 'clean'.

In investigations where the suspect is computer literate, these areas are sometimes used to hide information.

The actions of a suspect in removing or hiding evidence from a computer system can have the opposite effect, and strengthen the evidence. This is often the case with deleted files, or the non-destructive 'format' of the computer hard drive.

In PC-based operating systems, such as Windows XP and Windows 2000, there are a variety of 'cache files', 'swap files', 'audit logs', and 'registry entries' which all contain information about the actions of the user. An experienced computer forensic technician can quickly put together a profile of computer use, and identify potential evidence.

The two case studies in this section, though not themselves related to fraud, illustrate the power of electronic investigations.

Case study:

Investigation of defamatory 'Hotmail'

A large organisation was experiencing difficulties with the circulation of anonymous Hotmail email messages to its employees. The email included allegations which were defamatory to senior management.

A study of the email message headers identified the Sydney-based ISP to which the suspect was connected at the time the messages were sent. A search of company telephone call information stored by their PABX identified that one call had been made to this ISP from a telephone port within the organisation on the same day and during the same period in which the last Hotmail message was sent. The data port from which the telephone call was made was located in a communal area of a specific business unit within the organisation.

Computers were forensically imaged from this area. A series of keyword searches across the images identified one computer containing a reference to the Hotmail account in question. It was also identified that this computer had recently been de-fragmented, a process which can permanently destroy potential evidence.

The analysis

Detailed analysis identified data fragments that were attached to system files as 'file slack'. The keywords were found to be in fragments of HTML coding (the format used to write internet web pages). They were reconstructed and viewed through an internet browser. When reconstructed, the fragments were found to be internet graphic files which had been originally downloaded to the computer's 'temporary internet cache' (a temporary storage area for internet graphics which is designed to speed up access to internet web pages), but had since been deleted. The graphic files showed two separate web-based email accesses to the Hotmail user account in question.

The only way this information could appear on the computer is if the operator had used the username and password to access the Hotmail account from the computer. Time and date stamps associated with the text revealed that this activity took place prior to other employees of the company receiving the email from the offending Hotmail email address.

This evidence formed part of the grounds for the termination of the suspect's employment.

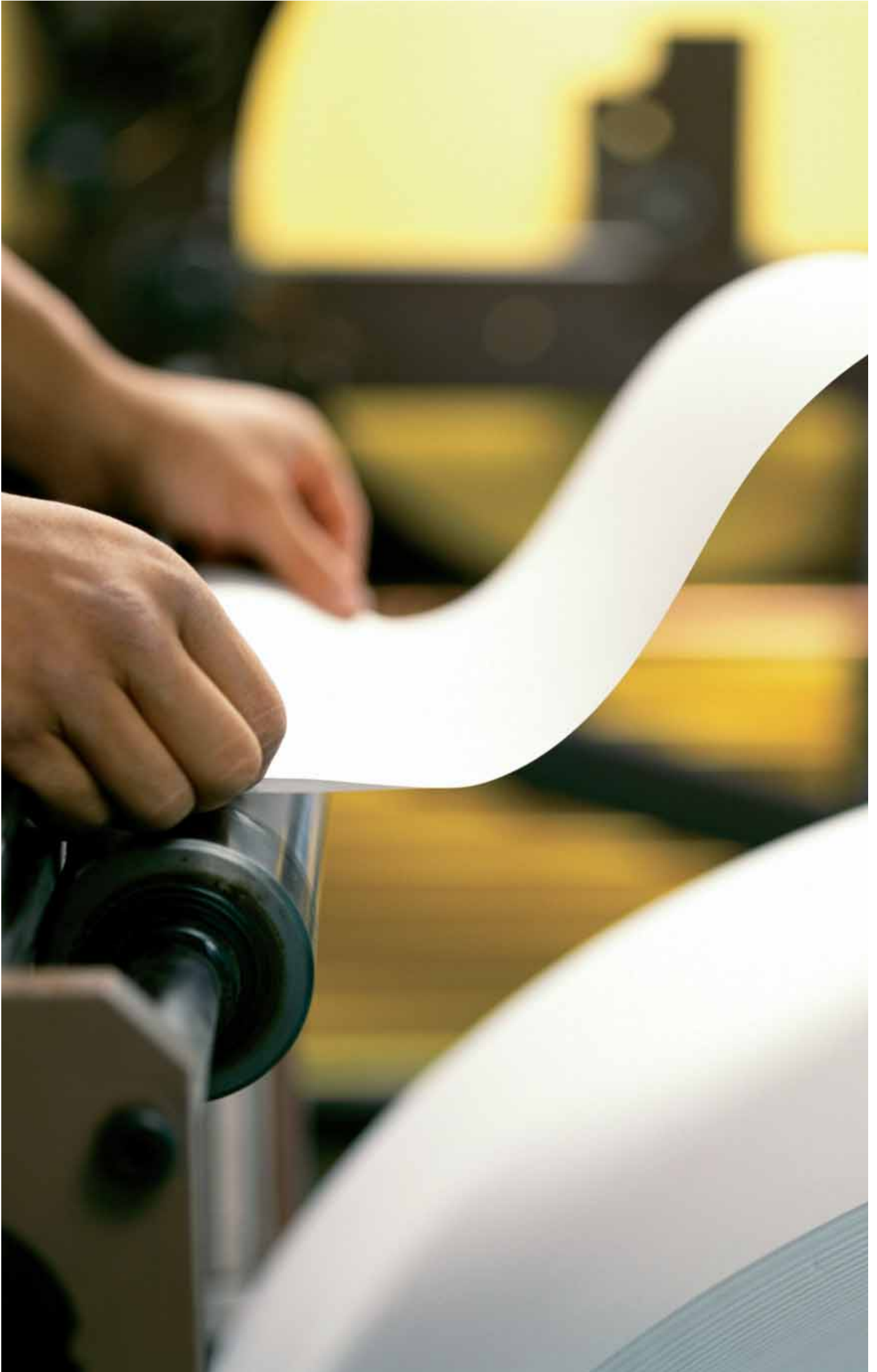
Subsequent investigation

However, in the weeks following the termination of employment, the anonymous email messages continued. This time the messages were sent to the organisation's clients, and threatened valuable contracts.

These messages were sent from an 'anonymous' web-based email site, which removes all information used in the tracing process. However the suspect was observed regularly using an internet cafe. A forensic examination of the computer system identified the messages sent and also recovered the evidence from a previous email message sent some four months earlier.

Result

Evidence collected through computer forensics was initially used to terminate the individual's employment. Further evidence was used to commence civil proceedings, which were quickly settled.



Financial statement misrepresentation

Do your numbers lie?

6

Revelations of accounting irregularities continue to make headlines. Many people shake their heads in disbelief and ask how did it happen and why wasn't it identified earlier?

The warnings from very public financial frauds, such as Enron and WorldCom, together with a tightening and regulator oversight has stemmed the tide of companies facing shareholder class actions relating to financial misreporting. However, alarmingly in the past two years, a company a week is still being sued for accounting irregularities and financial misstatement.

As illustrated below, the average settlement is steadily rising.

Accounting cases				
Year settled	No. of accounting related federal law suits	No. of financial restatements	Number of settled cases	Average settlement value (\$US)
1996-2000	106	49	161	18,600,000
2001	123	60	70	23,800,000
2002	167	82	81	17,400,000
2003	120	40	80	27,800,000
2004	132	51	78	34,800,000
2005	87	45	84	90,300,000
2006	64	37	77	74,100,000

These statistics are enough to keep Chief Executive Officers and Chief Financial Officers awake at night. Due to initiatives by governments and regulators around the world, they are facing potential criminal penalties and personal liability for unusual transactions in their company's accounts.

It is important to note that this is not just a US phenomenon. Australia has experienced its own financial collapses where allegations of financial misrepresentation have been made, and directors are not just facing civil actions for the recovery of funds, they are also facing criminal sanctions. The PricewaterhouseCoopers *Economic Crime Survey 2007*

identified that 14.1% of economic crime in Australia is attributed to accounting fraud.

Forensic accounting

Forensic accounting is a specialised discipline that arose to deal with instances of financial misstatement, in terms of both prevention and detection and, ultimately, recovery and remedy. Forensic accounting means the investigation or analysis of accounting evidence relating to unusual transactions due to either error or fraud.

Forensic accountants are generally used in two ways:

- to proactively investigate the control environment to identify weaknesses and areas susceptible to fraud or loss
- to investigate a specific situation to ascertain the true financial position where:
 - a transaction may have occurred but the cause is unknown, such as an unexplained loss, inventory variance or some other anomaly

– a transaction has been deliberately recorded to misstate the financial position.

Forensic accountants work closely with investigators in order to gather evidence to determine the facts of accounting transactions. These are often complex transactions, in an environment where there has been control breakdowns or weaknesses.



Case study: Inventory variance

A forensic accounting investigation of a product distributor's accounting records for suspected misstatement of \$40 million in inventory variances was undertaken. This included an analysis of suspense accounts to correct transactions, and to identify control weaknesses and control improvements to eliminate inventory variances.

Causes of the material inventory variance were identified which included improper accounting for product bundling, inventory returns and invoicing. In addition various unclaimed supplier rebates were identified that were recovered by the product distributor.

High risk areas for misstatement

The PricewaterhouseCoopers *Securities Litigation Study 2004* into US class actions revealed the primary reasons for misstatement of financial accounts, due to error or accounting irregularity, are:

- **Revenue recognition:** Two thirds of class actions arise from accounting issues associated with revenue recognition



issues such as: incomplete delivery of product; holding sales accounts open into the new year; billing customers but failing to complete delivery; over supplying customers to achieve sales with uncommercial rights of return offered through side letters; fictitious journal entries; backdating contracts; or falsifying documents and related party transactions.

- **Expense understatement:** for the first time in 2006 understatement of expenses was the highest cause of financial misstatement. Issues arose with respect to capitalisation of expenses, under provisioning of impaired assets, improper accounting for expenses associated with construction and in-progress assets.
- **Asset overstatement:** Issues often relate to estimates as to the adequacy of the provision for doubtful debts or uncollectable receivables; adequacy of warranty reserves or claim reserves; write-downs of assets; or adequacy of provisions for inventory obsolescence.
- **Understatement of liabilities or asset impairment:** Many cases relate to failure to record probable contingent liabilities and assets where the value and its impairment are difficult to estimate.
- **Inventory variances:** Sophisticated automated fraud detection programs should be used to analyse transactions, in order to identify unaccounted for inventory movements caused by bundling, receipting or invoicing errors. Diagnostics of inventory loss by type, territory, and timing to identify possible misappropriation or cause of loss should also be undertaken.

Case study:

Misappropriation by financial controller

The financial controller of a large organisation was alleged to have misappropriated \$5.5 million from the organisation through cheque fraud. An investigation was conducted to determine the extent to which amounts might have been misappropriated and to trace those funds to identify possible sources of recovery.

In addition, as a result of an attempt to disguise the misappropriation, various accounts had been misstated and liabilities had not been recognised. A full reconciliation of all accounts was conducted to determine the organisation's true financial position.

The misappropriated amounts were fully recovered from the perpetrator's assets, from a fidelity bond insurance claim, and a claim against the auditors for professional negligence. Accounts were reconciled identifying misstatement of assets and liabilities totalling \$8 million and various controls were implemented to reduce the risk of future misstatement.

- **Improper disclosure of transactions** especially in relation to contingent liabilities, guarantees and other company commitments.

Case study

Falsified schedule of value annexed to sales contract

A computer systems development company misstated its financial statements when one of its managing directors created a false schedule annexed to the sales contract where the contract amount was changed from \$13 million to \$20 million. The audit verified that the progress payments were receivable but did not verify the contract amount.

Red flags

A cry of disbelief is often heard when a financial misstatement occurs but often the same old red flags appear, including:

- inadequate or non-transparent explanations for unusual transactions, variances or results
- large adjustments made after period end. A comparison of the latest management accounts to year end accounts will help identify unusual variances such as increases in revenue or decreases in expenses.
- complex transactions that are not auditable, i.e. there is an absence of underlying documentation supporting the transaction
- creation of fictitious reconciling items to create the appearance that accounts are in balance, when they are not
- existence of concealment of documents, such as, 'side-letters' and other extra-contractual arrangements
- discovery of falsification of documents, dates (for example, backdating), contractual terms, or other business records
- significant related party transactions.
- unduly aggressive attitude by management towards financial accounting and reporting, especially market earnings forecasts
- lack of supervision and controls over decentralised parts of the organisation, such as overseas subsidiaries or regional offices
- rapid rate of change in the industry due to technological, competitive and other market factors, creating pressure to misstate the true financial position and/or enabling concealment of transactions in an unknown emerging environment
- failure of management to adequately address known internal control weaknesses; for example failure to implement recommendations of external auditors in management letters
- significant connection between earnings performance and management compensation such as bonuses or the contentious issue of options.

Simple strategies to mitigate risk

Organisations that experience problems with accounting policies can mitigate risk if they adopt and consistently demonstrate good corporate governance practices, as set out below:

Audit

- Internal Auditors who work independently of management and are potentially supplemented by an external independent adviser
- a special independent review of high risk areas such as revenue recognition

- accurate and informative reporting from management, for example forecasts that include detailed assumptions, actual results compared to those assumptions and any variations to forecasts explained.

Transparency

- the existence of an audit committee that meets regularly, invests sufficient time and resources, and is actively involved in reviewing key accounting policies
- transparency of material transactions through disclosure in the notes to the accounts, as required by International Financial Reporting Standards
- preparation of detailed and timely management accounts
- sign-off by senior accounting personnel that certain internal controls are being satisfied, such as reconciliation of key accounts including bank accounts and debtors.

Tone at the top

- It is often heard that the Chief Executive Officer directed that, no matter what, the company must reach certain numbers, such as earnings per share or Earnings Before Interest Tax Depreciation and Amortisation (EBITDA). Staff have interpreted this as an instruction to post fictitious journal entries to revenue or otherwise inflate revenue.
- Organisations that focus too much on one key performance indicator may tend to forget about others. For example, driving sales may help gross sales but this may be at the expense of the margin or quality of the debtors.

A fraud culture?

It is not just poor processes that result in internal control weaknesses, but also non-financial cultural factors (internal and external) which give rise to a higher risk of accounting irregularity. Such factors include:

- management's operating and financial decisions being dominated by a single person or small group of people

Case study: Bill and hold

A manufacturer felt pressure to achieve year-end sales forecasts and the sales force were asked to come up with strategies to meet targets.

One option taken was to 'bill and hold', where customers entered into a sale agreement for goods to be purchased but the product was sent to the manufacturer's own warehouse. Since responsibility for the goods was not passed to the customers there was no effective delivery.

The second option was to offer deep discounts to customers to purchase goods with a 'side letter' of guaranteed return, effectively creating a consignment, not sale. These transactions were identified through a review of the manufacturer's stocktake and unusual sales returns just after year end.

The manufacturer was forced to re-state its financial statements, the share price fell dramatically and the manufacturer and its senior officers faced regulatory action.

Culture

- The existence of a strong culture which fosters a two way communication of issues between leaders and staff. Where leaders express a reluctance to hear bad news, there is the possibility that staff will delay communicating problems until it is too late or the problem has become worse.

Forensic accounting process

Forensic accountants typically follow a standard process to gather evidence to identify financial misstatement, quantify any loss and determine options for recovery. This process includes:

- walkthrough/reviewing the purchase and sale cycles to observe and test controls to identify their effectiveness, including identifying non compliance and methods for

circumventing controls. Using an investigative mindset to challenge the control and experience of how past frauds have been committed, the forensic accountant often has a unique insight into where fraud risks might exist within these cycles

- reviewing and collating documents and electronic evidence related to the transaction
- interviewing staff to discuss fraud risk and instances of loss
- preparing a report which quantifies any loss and provides an explanation of the cause
- identifying opportunities for the recovery of that loss
- recommending control improvement to reduce the risk of future loss.

Company directors, especially Chief Executive Officers and Chief Financial Officers, are subject to increasing risk exposure, including personal liability for the actions and financial reporting of their companies. Yet how do you know whether the information you receive is sufficiently accurate, reliable, complete, relevant and timely to satisfy your duties and responsibilities as a company director? Important information you need to receive and review:

- liquidity reviews, including disclosure of cash balances and disclosure of restrictions on the use of cash and loan covenant compliance
- analysis of trade debtors, including a review of assumptions used to calculate provision for doubtful debts, collection trends and efforts to improve collections
- analysis of creditors, including analysis of aging and disclosure of creditors in dispute
- analysis of inventory, including a review of assumptions as to the adequacy of provision for inventory obsolescence
- analysis of earnings, including obtaining from management disclosures and analysis of the underlying assumptions and estimates in the preparation of management accounts
- analysis of forecasts for earnings and cash flow, including:
 - disclosure of underlying assumptions and changes in forecasts
 - comparison of forecast to actual results with explanation as to the nature of any variance
 - analysis of changes in underlying forecast assumptions
- other industry or company-specific reviews.

Conclusion

This guide is designed to give readers a broad overview of fraud prevention, detection and investigation techniques which have proved effective in the past. Naturally, some techniques will be more relevant than others, depending upon the industry and company involved. Organisations encountering fraud should take forensic and legal advice at a very early stage.

Taken together, these techniques should provide any organisation with an effective means of dealing with fraud risk.

About the authors

PricewaterhouseCoopers' Forensic Services Practice consists of approximately fifty staff across Australia, with backgrounds in law enforcement, civil investigation, computer crime and forensic accounting.

Many individuals have contributed to the content of this guide. Their contributions are greatly appreciated.

PwC Forensic Services contacts

For further information concerning the issues discussed in this guide, please contact the following partners:

Sydney

Malcolm Shackell

+ 61 2 8266 2993

malcolm.shakell@au.pwc.com

Cassandra Michie

+61 2 8266 2774

cassandra.michie@au.pwc.com

Melbourne

Steve Ingram

+ 61 3 8603 3676

steve.ingram@au.pwc.com

Robert Kus

+61 3 8603 6218

robert.kus@au.pwc.com

Brisbane

Ian Hall

+61 7 3257 8708

ian.hall@au.pwc.com

For more information about the specific Forensic Services provided by PwC, please visit www.pwc.com/au/forensicservices



