



Responding to Fraud

An ICAC discussion paper





Responding to Fraud

An ICAC discussion paper

**April
2002**



This publication is available in other formats for the vision impaired. Please advise of format needed, for example large print or as an ASCII file. It is also available in HTML format, at www.icac.nsw.gov.au

ISBN 0 7310 7259 6

© April 2002 – Copyright in this work is held by the Independent Commission Against Corruption. Part III, Division 3 of the *Commonwealth Copyright Act 1968* recognises that limited further use of this material can occur for the purposes of 'fair dealing', for example; study, research or criticism etc. However, if you wish to make use of this material other than as permitted by the *Copyright Act 1968*, please write to the Commission at GPO Box 500, Sydney NSW 2001.

Contents

Commissioner’s Foreword	5
Introduction	6
What is the purpose of this paper?	6
What do we mean by fraud?	6
What has happened to make fraud important now?	7
How do the changes affect agencies and councils?	8
How do we prevent fraud?	11
How we see it	11
Leadership	11
Risk Management	12
Guiding conduct	16
Staffing	17
Security	19
What do we suggest that agencies and councils should do?	21
What are your ideas and perspectives?	22
How to ensure early detection of fraud?	23
How we see it	23
Monitoring people	23
What do we suggest that agencies and councils should do?	26
What are your ideas and perspectives?	27
Monitoring transactions	27
What do we suggest that agencies and councils should do?	31
What are your ideas and perspectives?	32
How should organisations investigate fraud?	33
How we see it	33
Confidentiality first	33
Objectivity and impartiality	34
Assessing information	34
Reporting the matter to the ICAC	36
Who should carry out a fraud investigation	36
Planning an internal investigation	39
Formal investigation plan	40
Reconstructing transactions	43
Collecting and handling evidence	44
Interviewing witnesses	47
Interviewing suspects	52
Interview structure	55
Investigation reports	58
What do we suggest that agencies and councils should do?	61
What are your ideas and perspectives?	61

How should discovered fraud be managed?	62
How we see it	62
Setting the scene	62
Dealing with perpetrators	62
Preventing further fraud	64
What do we suggest that agencies and councils should do?	64
What are your ideas and perspectives?	65
What about these suggestions?	66
What to do with the answers?	69
Where did we get our information?	70

Commissioner's Foreword

The NSW Government has an annual budget of over \$30 billion. Council revenues from all sources amount to \$5.5 billion. Together, State and local government manage billions of dollars in resources. These resources are at risk if agencies and councils are not active, vigilant and effective in dealing with the risk of fraud.

Fraud is a crime. If a public official commits fraud on his or her agency or council it is also corruption. The NSW public sector does not escape fraud. It affects, or has the potential to affect, every public agency in the State.

The ICAC's job is to expose corruption and to build corruption resistance. This means that we need to help agencies and councils to deal with fraud. The best way to deal with the threat of fraud is effective prevention and strong detection measures. The best way to respond to suspicion of fraud is to investigate it thoroughly. The best way to respond to firm evidence of fraud is to ensure that it does not occur again and to attempt to prevent the culprit from getting away with it or doing it again.

Most frauds come from within organisations or with the assistance of people within. More sophisticated technologies such as the Internet, together with remote access to much of their data holdings, have increased the risk of organisations falling victim to an entirely outside-sourced fraud.

Fraud is also having a bigger impact on the community through the growing use of technology to access and manipulate data. The NSW Crimes Act now includes specific offences relating to data and computers. Simply gaining unauthorised access to data can constitute an offence.

All organisations need to ensure that they do all they can to protect their resources from fraud. A key part of that protective regime is ensuring that they respond effectively to evidence of fraud.

In 1998, the Premier's Department stated that major central and corruption prevention agencies should continue to improve standards of compliance with effective fraud control procedures. We are publishing this Fraud Response discussion paper to build on this work, particularly that of the Auditor General and the NSW Treasury. We also want to help organisations improve their capacity to investigate fraud. We think the time to do this is now. This is because the way fraud is investigated is changing. Agencies and councils are expected to take a greater role in investigating fraud. They can only do this if they have the right tools to help them investigate.

We are also asking for your feedback. We want to know if you think we have got the right approach. We want your suggestions on how we can make the final document better. We want to know if you think fraud is a big issue.

I hope you find our ideas useful. We welcome your input. All submission should be received by Monday 20 June 2002.



Irene Moss AO
Commissioner

Introduction

What is the purpose of this paper?

This paper reviews best practice in dealing with fraud. It looks at some of the challenges for the future. It has been published and distributed so that we can get peoples' ideas and comments on the right way to approach fraud.

Later in the year we intend to publish Fraud Response Guidelines. These will reflect the outcomes of this discussion paper and consultation process.

At the end of each section are a few questions that we would like you to think about and to discuss with your colleagues. We would then like you to tell us what you think.

We would also like your comments and suggestions on the broader issues that we have raised at the end of the paper. These issues are about the best way for State and local government to manage fraud risks in the future. We want to hear anything else you have to say about fraud and its management.

Please send us your comments. The contacts details are at the end of the paper. We need to receive your comments by close of business on Monday 10 June 2002.

What do we mean by fraud?

Fraud is a crime involving the dishonest obtaining of a financial or other benefit by deception. The benefit might be of direct value (e.g. money or easy access to money). It might be indirect (e.g. obtaining information by deception and then trading or using that information to obtain more tangible benefits). In contemporary financial transactions, no actual exchange of currency or even of documentation takes place. Data takes on a value equivalent to money.

The ICAC's primary interest is in preventing fraud that involves public officials. Members of the public who receive financial or other benefits from agencies and councils also sometimes commit fraud. Organisations should consider the information in this paper when developing strategies for dealing with this threat.

In this publication, we focus on fraudulent financial transactions. The ICAC is planning further work on other aspects of misappropriation such as misuse of resources.

Investigating and preventing fraud is a very important part of the ICAC's work. Principal officers of agencies and councils report incidents of suspected corrupt conduct to the ICAC. In 2000-2001, 10.9% of these reports related to "fabricating or falsifying information/fraud/forgery". In addition, 27.7% of reports involved the misuse of public resources. Much of this involved fraudulently obtaining these resources, since some degree of dishonest deception would be involved. This suggests up to 40% of the ICAC's business involves fraud.

What has happened to make fraud important now?

A 1999 KPMG survey of 1,800 of Australia's largest businesses (including government agencies) revealed that 57% had at least one incident of fraud in the two years prior to the survey. The government respondents had a slightly worse experience than the average, 62% had experienced fraud. And the average cost per organisation was over \$1.1 million.

So fraud control matters. Fraud control is a key element of good management in the public sector.

In March 1994 the NSW Audit Office published, *Fraud Control; Developing an Effective Strategy*. The publication was endorsed by the Premier's Department for use by NSW public sector agencies. It was also adopted by a number of local councils.

The NSW Treasury published its *Risk Management and Internal Control Toolkit* in September 1997. The toolkit is about more than fraud control. It provides important advice on establishing a framework for effective internal control and risk management. Using it, though, organisations can deal with fraud threats more effectively.

In 1998 the Audit Office reported that up to 80% of agencies still did not have adequate fraud control practices in place. In response it published "*A Self-Audit Guide for Assessing Best Practice in Fraud Control Strategies*". The Audit Office found some improvement in fraud control. But it argued more needed to be done.

The Audit Office advocates a ten-point strategic management model for fraud control. The ten points include a range of proactive and reactive strategies. The ten points identified by the Audit Office deal with detection and investigation issues. The model continues to be a valuable tool for organisations wanting to improve fraud control.

The Ten Point Strategic Management Model for Fraud Control.

1. Integrated Macro Policy for Fraud Control

Agencies should adopt a fraud control strategy. It needs to be holistic and complementary. It needs to be designed to meet the specific needs of the agency.

2. Responsibility Structures

Agencies need to define and communicate who is responsible for coordinating, monitoring, reviewing and promoting the fraud control strategy. It should not become the domain of elite groups.

3. Fraud Risk Assessment

Agencies should periodically conduct a structured fraud risk assessment covering all functions and preparations.

4. Employee Awareness

You need a programme to bring fraud control issues to the attention of all employees. It may include several strategies including training.

5. Consumer & Community Awareness

Agencies need to promote community awareness of their stance on fraud.

6. Fraud Reporting Systems

You need a set of procedures so potential complainants can notify the agency of possible fraudulent activity. It needs to be tailored to the size of your agency.

7. Protected Disclosures

Agencies need a policy on protected disclosures that makes it clear the agency wants people to come forward and report possible fraud and corruption.

8. External Notification

You need a clear policy on notifying relevant authorities such as the ICAC and the Police when you discover suspected fraud or corruption.

9. Investigation Standards

Agencies need procedures and guidance for staff on how suspected fraud will be dealt with. It is important that you have competent fraud handling and investigation procedures.

10. Conduct and Disciplinary Standards.

You need to make it clear that fraud is not tolerated and that perpetrators will be punished.

NSW AUDIT OFFICE (1999)

The NSW Police have always indicated that there needs to be sufficient evidence of fraud before it can act. It does not commit resources to suspected cases of fraud without such evidence.

But in early 2001, the NSW Police signalled a change in the fraud environment. The former NSW Police Commissioner Peter Ryan published a document entitled *NSW Police Service Future Directions 2001-2005*. Under the heading "My Plan for the Future" the Commissioner says that the NSW Police will carry out fraud investigations of major strategic importance as well as those involving entities or individuals lacking the resources to pursue such investigations privately. Most public sector agencies and councils will be seen as having the necessary financial resources to conduct fraud investigations themselves.

How do the changes affect agencies and councils?

Organisations need more than ever to get serious about fraud control. They are now expected to take a much greater role in managing fraud risks and in investigating specific instances of suspected fraud.

Agencies that have not taken greater responsibility to prevent and to detect and investigate fraud face two particular risks. Potential fraudsters may regard the risk of detection as lower. There may also be fewer effective investigations revealing the full extent of fraud.

Lower risk of detection

One of the main deterrents to individuals considering committing frauds is the prospect of being caught and the action that might be taken by the victims. Fraud is rarely a spur of the moment offence; it takes time to identify the opportunities, calculate the risks and rewards and determine that the risk is worth taking. As part of that calculation the potential fraudster may consider the likelihood and potential consequences of a Police investigation.

But the likelihood of a Police investigation is lower. Agencies and councils are now more likely to have to investigate fraud themselves. The potential fraudster should see the organisation compensating by increasing prevention or detection measures. If not, it follows that there is less deterrent to people thinking of committing fraud.

Inadequate investigation

A second major consequence of agency inaction relates to the adequacy of investigations. Where there is evidence of a fraud, the extent of that fraud, how it was perpetrated, the total value of the losses and the extent of continuing risks might not be revealed.

If an organisation does not gather enough intelligence about the threats to, and weaknesses of, its operations it will not be able to take appropriate and effective preventative measures. Investigation reports are an important source of intelligence.

Risks of poor fraud control

Agencies that are not vigilant in preventing, deterring, investigating and punishing frauds are at risk of a number of adverse consequences including:

- Damage to their reputation through perceptions of wastefulness and inadequate responses to fraud. The community expects that all agencies and councils will be efficient and effective. Where organisations are seen to be failing to protect public resources they risk losing the confidence of their staff the community, and of elected members of governing bodies
- Loss of revenue and increased costs. Undetected frauds frequently result in a steady loss of revenue, profits and other resources. This creates an appearance that the organisation is operating at reduced efficiency. Management decisions can be based on erroneous assumptions
- Reduced capacity to manage effectively. Measures to improve efficiency in organisations will be ineffective if they do not address the underlying causes of problems. If fraud is reducing revenue, stopping the fraud is the way to stem the loss

-
- Individuals perpetrating frauds doing other damage. Individuals perpetrating fraud, particularly serial frauds, are more likely to be devoting their energies and attention to the frauds and their concealment than to their actual duties. At any level of an organisation this can have serious consequences. At senior levels the effects can be quite marked
 - Damage to organisational culture leading to losses in other areas. The single most important influence on how well an agency or council functions is its underlying culture and values. An agency characterised by significant fraud cannot build a cohesive and effective culture. A negative culture is more conducive to other unacceptable behaviour
 - Costly litigation. An agency or council may fail to meet an obligation to a third party due, for example, to money or data being misappropriated. The agency may also be liable for any damage caused by such failure
 - Failure to meet the needs of good government. Ultimately all state agencies and local councils exist to meet the community's need for good government. They do so by providing services, regulation, information and the like. Where a fraud damages the capacity of an agency or council to deliver those services, it harms the community itself.

How do we prevent fraud?

How we see it

The best way to minimise fraud is good prevention and a credible detection regime. The best way to respond to increased fraud is to improve prevention and detection strategies. Agencies and councils can adopt a number of proactive measures to prevent the opportunity for fraud from arising. Steps can also be taken to minimise the risk of those opportunities being acted on. There is a wide range of preventative measures available. Some of those are outlined below under the following broad headings:

- Leadership
- Risk management
- Conduct guidance
- Staffing
- Security.

Leadership

The ICAC has conducted research into leadership and organisational culture. From the research, the behaviour of leaders is of great significance in fraud prevention. This is because staff copy what managers do rather than do what managers say. For example the research found:

- The most important thing in creating an ethical workplace is the behaviour of leaders
- The perception that leaders are honest is associated with staff having positive perceptions about colleagues, their job and the workplace
- Statements from the CEO on ethics have more impact on staff behaviour than do their own values.

Recognising this, the ICAC published *The first four steps: Building organisational integrity*. The publication assists agencies and councils to get the culture of their organisations right. It emphasises the importance of leadership.

Modelling behaviour

It is unrealistic to expect people to behave better than we do ourselves. Sound fraud prevention depends on leaders and managers clearly communicating their strong commitment to ethical behaviour. They should also model the behaviour they want staff to exhibit.

This means managers always saying and doing the correct things. People should see their leaders acting properly in a consistent manner. They can then be expected to behave similarly.

The First Four Steps to Organisational Integrity

1. Identifying a set of values for your organisation

Your agency needs to identify an appropriate set of values that will help you develop a better organisational culture. We suggest agencies work out what the prevailing culture is first. Use our Ethical Culture Survey Kit to do this. Then develop a new set of values.

2. Following these values yourself

Leaders need to set an example. It is important that leaders are always seen to be honest and to behave with integrity.

3. Promoting these values to others

You can talk about values and ethics to your staff, clients and other organisations. Promote values to staff by telling stories, making ideas concrete, using awareness programmes and building ethics into training.

4. Building integrity into every decision and action.

Organisational integrity needs to be fully integrated into the workings of the organisation. There are lots of tools to achieve this. Codes of conduct, internal controls, performance management and ethical procurement policies are some examples.

Risk Management

Risk assessment and planning

Agencies and councils manage valuable public resources. They are expected to ensure these resources are used to meet the needs of the community.

Organisations face risks in managing public resources, including the risk of fraud. As those risks cannot be avoided entirely, they must be managed. A managed approach involves a number of strategies.

Risk management is now a mandated part of good practice in the public sector. The *General Government Debt Elimination Act 1995* sets out fiscal principles by which the Government must pursue its objectives. Fiscal principle 6 is to manage debt in accordance with sound risk management principles. The Act states each government agency must produce and maintain a risk management plan.

The *Annual Reports (Departments) Act 1985* sets out what each Department's report of operations must contain. The report must include a report on risk management and insurance arrangements and activities affecting the Department. Treasurer's Direction 900.01 contains matching provisions. It makes authority heads responsible for risk management and insurance and calls on them to report on these matters in the agency's annual report.

Risk management committees

Risk management committees have overall responsibility for risk management. Sometimes an audit committee performs this role. All organisations should have a body with responsibility for risk management, particularly for fraud control. It is part of having a good fraud reporting system. A risk management committee is also a good source of advice on building an integrated approach to fraud control.

Risk management committees can be responsible for:

- Developing all risk management plans
- Ensuring that the plans are implemented
- Monitoring the effectiveness of the plans
- Reporting to senior management on risk issues
- Ensuring that fraud risks are identified and acted on
- Supervising investigations.

Function and position risk profiling

To get a clear picture of your organisation's fraud risk profile you should identify all of its activities. These are then assessed for the likelihood of a fraud being perpetrated and for the extent of the damage or loss that would be involved.

A picture emerges of the areas of fraud risk and the weaknesses in those areas that need to be addressed. This is a prerequisite for addressing the threats.

Fraud risk management plans

It is important that the management of all risks within an organisation be integrated. This is because all types of risk management have in common the protection of the organisation's interests. But sometimes they appear to have conflicting concerns. The key is total risk management. An important part of total risk management is fraud risk management.

Organisations have a number of options in managing a fraud threat. These include:

- Shedding the risk entirely by discontinuing an activity where the benefit is not seen to be worth the risk
- Sharing the risk by entering into joint service provision arrangements or by taking insurance
- Reducing the risk by taking pro-active measures, many of which are described in this publication.

For example, organisations dealing with significant amounts of cash can reduce risk by giving customers incentives to pay other than by cash.

Corporate fraud risk management plans draw into a single document fraud risk assessment, potential damage projections and identified reduction strategies for all high-risk transactions throughout the organisation.

That document identifies the:

- Risks
- Actions to be taken
- Arrangements made for managing those risks
- Methods for monitoring the effectiveness of those strategies
- Individuals responsible for implementation and monitoring of each aspect of the plan.

Data collection and analysis

An organisation's fraud risk management plan sets out who is responsible for implementing strategies for preventing or detecting anticipated fraud.

But not all frauds can be anticipated. Sometimes people see an opportunity to defraud an organisation that nobody else has noticed. These opportunities may not be identified in your fraud risk assessment.

So organisations need redundant or secondary measures for monitoring their activities. These secondary measures should involve monitoring trends, activities, complaints and compliments for signs of irregularities.

For example, an increase in the frequency of break down of motor vehicles or other plant may indicate that:

- Maintenance is being paid for but not performed
- Equipment is being used for additional unauthorised work
- Unqualified operators are being used
- Additional equipment apparently being hired is not being used.

Procedural provisions and record keeping

These serve to keep management informed of trends in business and to guide supervisors procedurally. They are different from risk management strategies because they are part of an organisation's overall business monitoring activities. They do have important fraud risk management features.

Audit plans: All organisations should conduct a full organisational survey to identify all of the transactions they are involved in. They should then apply this information to develop a comprehensive audit plan that monitors those transactions. They should cover key financial risk areas including payroll, purchaser and supplier systems, petty cash and other cash handling activities.

Audit trails: All work practices, project plans and procedures should have auditable features included in their design. Staff should be encouraged to recognise the value of ensuring that the nature and reasons for all their decisions are recorded and accessible for audit. This is particularly so for those involving fraud risks.

'At Risk' Occupations: Most organisations have positions that present the opportunity to participate in fraud. Other positions are vital to fraud detection.

Indicators of high-risk occupations include those with high degrees of discretion and those making decisions that have high cost or reward impacts.

You should ensure that occupants of the positions are:

- Frequently rotated between duties, territories, suppliers or customers
- Regularly involved in individual discussion with supervisors about their duties and relationships
- Properly supervised
- Monitored to ensure they follow procedures.

The risk management committee should have overall responsibility for ensuring the continuing effectiveness of procedural provisions and record keeping arrangements.

ICAC investigation reports

A good source of advice on dealing with fraud risks is the work of the ICAC in this area. Up to the end of 2001, the ICAC had published 87 investigation reports. All contain details of corruption allegations. Most of them contain recommendations for making organisations more corruption resistant. They include recommendations dealing with fraud.

The lessons of these investigations do not apply solely to the agencies involved. They should be taken into account by all agencies when they are doing risk analyses or considering the dangers of engaging in risky ventures.

For example, in June 1999 we produced *Weighing the waste: an investigation into conduct at local council waste depot weighbridges at St Peters and elsewhere*. This should be studied by any organisation that operates waste facilities. It outlines some control measures to prevent fraud at tips.

In November 2000 we produced, *Rebirthing motor vehicles: investigation into the conduct of staff of the Roads and Traffic Authority and others*. This investigation report contains material useful in dealing with the risk of identity fraud.

All published ICAC investigation reports are available through the Commission's web site:
www.icac.nsw.gov.au.

Further reading

For a comprehensive introduction to risk management, see the *NSW Treasury's Risk Management and Internal Controls Toolkit* (NSW Treasury, 1997)

Another good source of advice on comprehensive fraud risk planning is the *Commonwealth Fraud Control Policy and Guideline*.

Most work in the area is designed to comply with Australia/New Zealand Standard AS/NZS 4360:1999 – Risk Management.

Guiding conduct

Code of conduct

An effective code of conduct should guide behaviour in the workplace. To be effective a code of conduct should be continuously promoted. It should be used as a practical guide to day-to-day behaviour and decision-making. It needs to be supported in ways that are consistent with the broad behaviour it promotes. This is done by:

- Management commitment
- Appropriate training
- Awareness programs
- Systems, policies and procedures.

Conflicts of interests

Everyone who works for an agency or council has a duty to serve the public interest and to avoid serving any private interests in preference to public interests. Where public officials have, or seem to have, a private interest in a matter they become officially involved in they are said to have a conflict of interests.

Fraud is a corrupt outcome of a conflict of interests. The conflict is between the public interest in ensuring that its resources are honestly applied to the public benefit and the individual's interest in obtaining a benefit by deception.

Allegations of corruption often arise because of perceived conflicts between the public interest and private, professional or commercial interests. This makes understanding and managing conflicts of interest an important aspect of building an organisation's fraud resistance.

Agencies and councils should ensure that sufficient guidance is in place to help staff identify and deal appropriately with conflicts of interests.

Further reading

Advice on conflicts of interests is available in the Premier's Department's Model Code of Conduct (1997) and in the Department of Local Government's Model Code of Conduct (1994). The ICAC publication *Under Careful Consideration: Key issues for Local Government* covers many difficult issues in conflicts of interests. The ICAC's new publication on codes of conduct, *Codes of Conduct: the next stage*, will shortly be available. Both ICAC publications are available on our website www.icac.nsw.gov.au

Gifts, benefits and bribes

Gifts, benefits and bribes are usually intended to influence the way the recipient carries out official functions. It may be to dissuade the recipient from looking too closely at a fraud, to look away when it is identified or even to actively participate in fraud.

Exposure to offers of gifts, benefits and bribes is almost inevitable among staff who:

- Provide customer or client service
- Procure goods or services
- Carry out regulatory work
- Carry out any work with the private sector.

A gifts and benefits policy and procedure is an important part of an organisation's fraud resistance framework.

Further reading

The ICAC published a comprehensive guide on gifts. It is called *Gifts, Benefits or Just Plain Bribes*. Like all our publications, it is available free of charge on our website: www.icac.nsw.gov.au.

Staffing

Recruitment and verification

Recruitment presents the first opportunity for organisations to assess a person's risk potential. It is a good time at which to look for indicators. The individual is not yet employed. A difficult risk situation can be avoided by not engaging at-risk individuals in at-risk occupations. It is also a good time to get information about their personal circumstances for monitoring purposes.

Similar opportunities arise when a person is being considered for promotion or transfer.

Questioning, contacting referees and verifying written claims of qualifications and experience should verify information that is provided at a job interview.

Forged qualifications are now readily available through the Internet or easily manufactured on a home computer. If such documents are important to establishing the candidate's suitability, they should be checked.

You should watch for any indication that a candidate is dismissive of the importance of ethical conduct, or otherwise shows a disregard for the probity aspects of their duties. This should be considered in the context of fraud risk management. It may indicate that they pose a potential fraud risk.

Staff training

Staff who have been well trained, know their jobs and are confident in their abilities, tend to enjoy their work. They are less likely to commit fraud and more likely to report wrongdoing. They are also more likely to notice when fraudulent transactions are being carried out. This is because they are better able to tell when the rules are being broken.

Staff in high-risk areas should also be trained in fraud detection and in how to report signs of fraud when they appear. Those indicators are discussed below.

Training should include recognising:

- Counterfeit currency
- Forged or altered documents
- Inconsistencies in details provided
- Unusual demeanour.

Internal reporting

An effective internal reporting system is a valuable mechanism for detecting fraud and identifying suspicious behaviour in the workplace.

Agencies and councils should develop an internal reporting system that encourages staff to report anything that they note in the workplace that they think is suspicious. The range of matters that should be reportable under an internal reporting system should be much wider than those involved in protected disclosures (see below). They should encourage a steady flow of information, which might assist in the early identification of fraud or fraud risks.

In encouraging staff to report suspicions it is important to remember the presumption of innocence. Staff who report suspicions of fraud should not be led to believe that a person will automatically fall under suspicion or be punished.

Protected disclosures

The *Protected Disclosures Act 1994*, supported by an internal reporting system, supports the community's interests in probity in public administration.

The Act provides protection for people who report corrupt conduct, maladministration or serious and substantial waste. If an agency or council has an internal reporting system for the purposes of the Act, it is possible for staff to make protected disclosures internally and obtain the protection of the Act.

Encouraging protected disclosures is an effective fraud prevention tool. Protected disclosures can provide information on frauds being perpetrated or circumstances that create the opportunity for frauds to occur.

Further reading

The NSW Ombudsman has produced a comprehensive guide in this area - the *Protected Disclosures Guidelines* (4th edition, 2002).

Grievance management

Fraud is sometimes motivated by revenge. Organisations must ensure that grievances are dealt with quickly, confidentially and effectively. The risk of disaffection leading to staff committing fraud, or being less likely to report it, is significant.

Industrial relations

It is always important to ensure that industrial relations are properly managed. A good industrial climate in an organisation is linked to good morale and a healthy ethical environment. A poor industrial environment hinders detection and investigation of fraud. Industrial problems can arise when preventative steps affect individual staff members.

For example, objections might be raised to steps taken because a person is assessed as presenting a risk. People may want their unions to intervene where they are to be:

- Moved to different jobs
- Moved to a different location
- Interviewed about aspects or indicators of concern
- Deprived of certain responsibilities
- Denied relieving opportunities.

Objection might also be raised to steps being taken as a result of the detection of an actual fraud where no perpetrator has been identified. For example, they can arise when everyone who worked in an area that suffered a fraud is transferred.

Organisations need to involve staff associations and unions as partners in fraud risk management. Agencies and councils need strategies that are fair and will be in the interests of staff and their organisation generally. All parties must accept that the community expects that agencies and councils will not tolerate fraud.

Further reading

Many of these issues are covered in the Auditor General's *Fraud Control: Developing an Effective Strategy (1993)*.

Security

Information security

Many frauds involve obtaining information by deception and then using that information to obtain more tangible benefits. Data is taking on a value equivalent to cash. It can also be converted to, or used to obtain, cash.

Insiders perpetrate most frauds. Organisations are also at risk of fraud via remote telecommunications access. Fraud over the Internet can be perpetrated:

- From distant sites in other jurisdictions
- From masked locations
- By masked identities
- In a short time
- In ways which can delay detection for some time
- By means which are novel and constantly being improved.

Protecting electronically stored data is a challenge of the times. The data must be protected against unauthorised access from within and also from outside. Some things that can be done to guard data holdings:

- Organisations need to make clear risk based decisions about who has access to what data, and to what level. Banking and payroll systems are especially sensitive and need to be protected from improper access.
- Everybody who accesses data should be issued with a unique login identification. In conjunction with a password, this should be required for all accesses
- Logins and passwords should be used so you can tell when data is accessed, updated, amended or deleted and by whom. They must not be used by more than one staff member and should never be shared
- Passwords that contain both alpha and numeric characters are much harder to break. This is because they offer many more combinations than those only containing digits or letters. They should be used wherever practicable
- All accesses to data should be recorded and available for monitoring. Records should also be available for audit
- Staff should ensure that unattended computers are locked or logged off.
- You need to make it clear using another officer's password will not be tolerated. This should be dealt with in the organisation's disciplinary arrangements, training and induction
- Passwords should be regularly changed. They should also be changed when a person thinks someone else might have found out their password
- Organisations need to provide electronic access for branch offices, field staff, customers and the community. Firewalls protect agencies from unauthorised access from outside
- Organisations need to access to their data holdings in order to operate. This makes them vulnerable to extortion through the threat of "denial of service" attacks. These occur where an organisations systems are manipulated from outside in such a way as to prevent it from functioning. It is necessary to develop a contingency plan setting out what will be done, and by whom, in the event of a denial of service attack.

Physical security

While fraud always involves a degree of deception, it can also involve a physical dimension:

- Cash must be carried away by some means
- Data might be accessed directly in the workplace thereby circumventing access controls such as firewalls
- Hard records might be accessed or copied out of hours or by unauthorised persons
- Documents containing confidential information may simply be left lying around and be discovered by opportunists.

There are also a number of organised groups and individuals who simply move around business districts and office buildings looking for opportunities.

They look for poorly secured information such as accounts, credit cards or credit card receipts, or order form numbers. They can use this information to perpetrate frauds against the organisation or members of staff. Documents such as stored cards, cheques or order forms can be stolen and fraudulently negotiated.

Organisations need a system to deny access and to monitor and record who has access. Access denial involves active access control. Organisations need to control access to resources so that they can be used legitimately. Access controls should give authority to enter premises and to enter any part of premises. The system records such movements. This helps to detect, as well as deter unauthorised access to premises.

Video monitoring allows for passive monitoring of movements of individuals and vehicles. This permits organisations to monitor movements around and activities within premises. Awareness of video monitoring can be a significant deterrent.

Access controls and video monitoring should be regularly promoted to staff and customers alike as a means of maintaining their deterrent effect.

It is necessary to make sure everyone practices sound individual security. This means securing any items that might be of value to an intruder. Secure such things as chequebooks or forms, accountable forms, receipts, lists of accounts and their numbers. Particular care should be taken to secure access codes including passwords and account and credit card PINs.

What do we suggest that agencies and councils should do?

- Ensure that all managers and senior staff provide leadership by ensuring that their behaviour at all times reflects the standards that are expected of all staff
- Establish risk management committees or ensure that another clearly identified body has overall responsibility for risk management
- Carry out comprehensive fraud risk assessments and develop plans for addressing each identified risk
- As part of the risk assessment, develop profiles of all functions and positions for planning purposes
- Develop fraud risk management planning documents that identify:
 - Risks
 - Actions taken and arrangements made for managing those risks
 - Methods for monitoring the effectiveness of those strategies
 - Individuals responsible for implementation and monitoring of each aspect of the plans
- Put suitable arrangement in place to collect and analyse intelligence data concerning at risk areas of the organisation and its activities. These should include individual login codes and passwords
- Refer to ICAC investigation reports for information concerning the experiences of others
- Have a code of conduct that is fully understood by all staff and provides guidance as to how they should conduct themselves in the workplace and while carrying out their duties

-
- Regularly review the code of conduct
 - Ensure that breaches of the code of conduct are acted upon
 - Adopt a suitable policy concerning gifts, benefits and bribes
 - Ensure that they find out enough to set a baseline about the personal circumstances of people before they are hired, promoted or transferred
 - Train all staff in all aspects of their jobs including fraud prevention and detection
 - Put in place an internal reporting system that maximises the likelihood of frauds being reported
 - Give staff confidence in reporting fraud and other inappropriate conduct under the *Protected Disclosures Act 1994*
 - Establish grievance management systems that allow personal problems in the workplace to be quickly identified, addressed and resolved
 - Ensure that staff associations and unions are fully aware of the organisation's position on fraud
 - Make staff, staff associations and unions aware of the steps that will be taken to investigate suspected fraud and how perpetrators will be pursued when fraud has occurred
 - Ensure that individual work practices assist in fraud prevention
 - Adopt policies and procedures specifically designed to protect data holdings from unauthorised access, amendment or denial of service
 - Ensure that the physical environment is controlled and monitored in order to maximise fraud resistance, detection and deterrence
 - Arrange for all work practices to include sufficient record keeping to be readily monitored, audited and policed
 - Identify, and arrange for the close monitoring of all positions and work locations that are at high risk of exposing the organisation to fraud.

What are your ideas and perspectives?

Do you think the features listed here are important in fraud prevention?

Are there other things that you think should be included?

Does the size of an organisation have an affect on how it can work to prevent fraud?

Do you think fraud deserves special attention compared with other forms of corruption?

How to ensure early detection of fraud?

How we see it

It is critical to a successful fraud risk response strategy that organisations detect fraud as early as possible. Investigations can then be initiated and remedial steps taken to protect the agency or council and its assets.

Sometimes it is necessary to allow a fraud to continue. This is so that it can be investigated. This allows sufficient evidence to be compiled and all perpetrators to be identified. It also allows for the identification of the means they employed and of weaknesses in systems.

When organisations find evidence of fraud it should be treated as highly protected. It must not be assumed that it is a case of having found a “rotten apple” and so lift the confidentiality too soon. To do so would risk warning off other perpetrators.

The problem with the “rotten apple” approach to fraud is that it results in an incomplete investigation. If organisations believe that nothing else is wrong and that remedial steps are unnecessary, then they may overlook the full scale of the fraud, deficient systems, and poor culture.

Staff who suspect that fraud is being perpetrated in an organisation must know how to report it. They must also have confidence that they will not suffer from reporting fraud. They must also feel confident that something will be done with their report.

While fraud will occasionally be detected by chance, organisations cannot rely on luck to protect them from fraud.

Monitoring people

The 1999 KPMG fraud survey found that 57% of fraud was committed by non-management employees, 21% by managers and 22% by external persons. Insiders, employees and managers of organisations perpetrate most frauds. Most fraudsters are trusted employees who occupy positions from which they can carry out fraud undetected. Usually they seize the opportunity when it presents itself and appears to be a worthwhile risk.

Most people are not inclined to commit crimes, including fraud. But if the circumstances arise, some will take advantage of the opportunity to gain a benefit. The main conditions that need to be met are:

- An opportunity
- Inclination driven perhaps by need or by greed
- The capacity to give themselves permission to act, perhaps derived from underlying resentment
- A belief that the chance of being caught is worth the risk.

Formerly trustworthy employees may take advantage of opportunities to commit fraud. Some even go out of their way to find opportunities. This can happen even in organisations with very good fraud prevention arrangements.

When these circumstances arise, people can become a risk to their organisations and to themselves. Organisations need to be vigilant in knowing the signs that a staff member is becoming a risk.

The following table sets out a number of risk areas and the indicators to look out for in employees and colleagues in high-risk areas of your organisation. If any of these indicators appear they should be viewed as “red flags” or danger signs. Staff who have previously noticed “red flags” have later drawn these to the attention of ICAC investigators. It would have been better if they had been reported sooner.

These indicators do not prove that a person is committing, or is about to commit, fraud. But they do indicate that a risk is emerging that needs to be managed.

Organisations need to know enough about the personal circumstances of staff to be able to verify the “red flags” when they seem to appear. It is a good idea to review these circumstances from time to time. This is more important in the case of staff in high-risk positions. But this is a complex issue and must be handled with sensitivity.

One way to raise these sensitive issues is to program confidential discussions with individual staff. This can be part of a regular review process. It will give staff an opportunity to raise any concerns without arousing the suspicion of possible fraudsters.

Risk indicators

RISK	INDICATORS
General Circumstances	Excessively familiar with regulated entities Not rotated through jobs, territories, responsibilities Captive of customers or suppliers Exercises delegations alone Resists accountability arrangements Resists work/organisational studies Under-supervised Too trusted Personal relationships in workplace Contacts outside work Apparent windfalls bringing wealth
Interests	Lots of status symbols Spending too much Excessive use of alcohol or other drugs Excessive gambling Prurient interests

RISK	INDICATORS
Behaviour at work	Keen on overtime Does not take leave Erratic attendance patterns Does not share information Refuses career advancement opportunities Shunned by colleagues Supervisory pressure
Morale	Salary dissatisfaction Not feeling valued Appears grasping financially Tends to manipulate systems to advantage Unchallengeable type
Personal problems	Showing signs of excess stress Sickness in family Marital difficulties Too much debt Financial hurdles

Fraud rarely occurs entirely out of sight. Usually someone notices changes in a person's behaviour. Supervisors, in their day to day interaction with staff, may notice behavioural changes in individuals.

Organisations should have some way of reporting these observations in confidence. The risks associated with the behaviour must then be assessed and managed appropriately.

Organisations should be able to respond in a number of ways when "red flag" indicators emerge. These include:

- Counselling
- Training
- Job rotation
- Changing roles
- Changing procedures
- Removal of responsibility
- Changing location
- Requiring behavioural modification
- Changing client base
- Separation from the organisation.

Identity verification

We have looked at monitoring people who want a job. This is to ensure they are who they say they are. But it not just potential staff who pretend to be something or someone they are not. Identity fraud is a major problem and a growing one. Valuables, documents or data can fall into the hands of anyone who has passed themselves off as someone they are not. The perpetrator is unlikely to be caught.

It is now possible to forge almost any document including driver's licences, passports and birth certificates. The forgeries are all but undetectable to the untrained eye. This means that the traditional ways of identifying people are not now enough.

Documents will still be important to the identification process for some time to come. This is because presently available alternatives are too slow, cumbersome, expensive and unreliable.

Agencies and councils need to develop ways of independently verifying that documents on which they rely are genuine. This usually means approaching the issuers of documents. They can assist in verifying documents. Intentionally delayed delivery of services or access might permit a more thorough examination of all documentation tendered.

Agencies and councils need to be rigorous in setting and maintaining standards that will protect them from identity fraud.

What do we suggest that agencies and councils should do?

- Train all supervisors and staff in:
 - Risk management
 - The value of early intervention
 - How to identify risk indicators
 - What to do when they are observed.
- Ensure that they have systems in place to respond swiftly and effectively when risk indicators are observed to be present
- Ensure that the amount of information held concerning members of staff is sufficient in light of their position's risk profile
- Conduct regular reviews of the personal circumstances of staff
- Ensure that supervisors are able to note early signs of risk indicators and respond appropriately
- Allow for regular confidential conversations with all staff that include discussion and observations of the behaviour of colleagues about whom they hold reasonable concerns
- Ensure that the workplace is monitored to identify and deal with the emergence of risk indicators
- Have procedures in place for monitoring at-risk individuals or circumstances
- Verify important background information provided by job applicants prior to their being placed in positions of trust.

What are your ideas and perspectives?

Do you think the features listed here are important in fraud prevention?

Do you think it is fair to assess people from the point of view of fraud risks?

Have you any suggestions for other ways of identifying people risks?

Have you any suggestions for other ways of managing people risks?

Can people risks be handled confidentially?

Monitoring transactions

A transaction is any activity in which any of an organisation's information, tangible or intangible assets or resources, services or facilities is accessed, used, transferred, amended, created or destroyed.

All organisations should monitor all of their transactions as closely as possible. This is so that they can remain effective.

Transaction capture, or ensuring that no transaction goes unnoticed or unprocessed, is at the heart of all business management systems. It is also at the heart of fraud control and detection.

Transaction capture alone is not enough. It is also necessary to monitor transactions. This is to ensure that the responsible staff are complying with policies and procedures.

Routine verification

All accounts, bills, invoices and other sundry demands for payment received by an organisation must be checked. This process should involve at least two people. One should verify the expenditure was incurred. The other should ensure that the expenditure was properly authorised in the first place and authorise payment. The same person should never incur expenditure and authorise the payment of a resulting account.

There are dangers in setting threshold amounts below which transactions need not be properly verified. Organisations are vulnerable to the practice of "skimming". Credit cards numbers can be used to conduct many small, fraudulent transactions. These appear on statements but can go undetected as they get below an organisation's "money radar".

False pro-forma invoices can siphon away assets. Documents that appear to be genuine demands for payment for goods or services received can be routinely paid to avoid the cost of verification.

Refunds and nil-amount transactions also present risks. Instances of these should be checked and authorised by a second officer. This involves using what are called exception systems. You should ensure there are matching checks, logs and other auditable records. Unusually high numbers of refunds and cancelled transactions may indicate there is a problem. A background system to monitor these kinds of trends is a very useful tool if your organisation processes lots of transactions.

Cash handling is a risky activity that virtually all organisations must manage. Treasurer's Direction 440.01 provides that authority heads should designate an officer to be responsible for operating security devices and developing security regime in offices that handle cash.

Credit cards drawn on corporate accounts are a major risk. Senior staff who are seen as trustworthy individuals able to judge when credit cards should be used are more likely to hold these. Audit and account staff are often junior to card holders.

As stated above, 21% of frauds against organisations are by managers. It is important that corporate credit card accounts are never certified or approved for payment solely by the cardholders. There is usually less supporting documentation explaining the reasons for incurring expenditure.

All credit card accounts should be checked to ensure that all expenditure was incurred properly and is certified to that effect. Certification should be done first by the cardholder and then by another officer not in a line relationship with the cardholder. A third party should then approve the actual payment.

Performance assurance

Organisations can be deceived into making payments for goods or services that are not fully delivered or performed.

For example, specific purpose grants made to non-government agencies such as charities or community groups can be misused unless performance is monitored. A funded course of study may go undetected while funding is retained unless the funding agency verifies performance.

It is important to closely monitor the use of such funding. Options include:

- Requiring regular detailed reports,
- Disbursing funds over a period rather than all at once,
- Requiring that accounts be forwarded to the funding agency for payment
- Maintaining regular contact with the recipients.

Internal Audit

A large number of the matters reported to the ICAC by agencies and councils involve fraud uncovered by an internal audit. Internal audit is a vital part of an effective internal control regime.

Internal audit provides systematic scrutiny of an organisation's operations, systems and performance. It also provides management with a wide range of information and recommends ways that organisations can be managed more effectively. The internal audit function is an important fraud prevention strategy. It helps organisations effectively monitor their transactions.

Samples of transactions should be regularly audited. Audit findings should be developed into recommendations for remedial action. Internal audits need to become part of routine management monitoring. Such monitoring should also incorporate regular reviews of audit outcomes.

One of a local council's biggest risk areas is preserving its rates income. One effective strategy to minimise the risk of fraud is to reconcile income received and owing from rates with land classification and the Valuer General's land values for the council area. This should indicate whether you are receiving the correct rate income. If it is not at the right level, then you can investigate further. This type of reconciliation is an important part of a good audit plan.

Un-programmed checks

Sometimes the perpetrators of frauds make allowance for routine internal audits. So they design their activities to avoid detection by programmed checks.

The predictability of programmed checking of captured transactions can be a problem. For example, programmed checks may miss shortfalls in stock or valuables that have been temporarily made up to make it appear that all is in order.

To address this, in addition to frequent programmed audits, random checks should be conducted. Agencies and councils should consider the level of fraud risk and the potential losses involved as factors determining the frequency and depth of such checks.

Internal reporting

People in organisations notice much more than they report. During an ICAC investigation we executed search warrants on a person's workplace. A number of his colleagues came forward and reported that they had long held suspicions about him. They said his work practices, excessive lifestyle and modest salary were hard to reconcile. Had they reported these "red flags" the fraud might have been uncovered sooner.

For an internal reporting system to be effective people must know about it, understand what might constitute fraud and understand why it must be exposed. They must also feel confident that reports will be acted on and that they will be protected from retribution.

Further reading

Treasury Direction 720.01 states that authority heads must ensure there is an effective system of internal control in place for their agency. Clause 13 of the *Local Government (Financial Management) Regulation 1999* makes the General Manager responsible for establishing an effective internal control system.

The NSW Treasury *Risk Management and Internal Control Toolkit* will give you a lot of help in reviewing and improving your internal audit and internal control regimes.

Customers as monitors

Many frauds are uncovered as a result of complaints from customers. For example, if money is collected but the transaction is not recorded properly the customer may receive a further demand for payment.

This is less likely with cash transactions where no receipts are issued. For example, using a swimming pool or waste depot is unlikely to result in a reminder notice for non-payment. So agencies can turn customers into fraud detectors. There are a number of ways that this can be done.

Cash registers display to the world the record of a transaction. You can encourage customers to check that the correct amount is displayed. This check is to ensure that the correct amount has been charged. But the check also ensures that the transaction is recorded.

Organisations can make it in their customers' interest that transactions are properly recorded. Spot checks of receipts should be made inside venues. If penalties are imposed where receipts are not produced, customers will make sure they get a valid receipt. The checks and penalties should be made clear to the customers.

Another way is to monitor customer experiences. This can be done by writing to a sample of customers asking them relevant questions about a service. For example they might be asked about:

- Receipts issued
- Discounts given
- Observations they made
- Improvements they suggest.

It is a good idea for customers to know about fraud, and why it is important that it be exposed. Again, people must feel confident their report will be dealt with properly and that they will be protected from retribution.

Reconciliation of information

Organisations often receive complaints and other information from the community. Agencies and councils should always try to identify what in fact occurred even when their preliminary inquiry is inconclusive.

Say a person complains of not receiving a service for which they paid cash but received no receipt. It is not sufficient to establish that there was no surplus on the day, that the receipt books are intact and that nobody involved remembers anything untoward. An unrecorded transaction has occurred. It may or may not involve fraud. Unless a satisfactory explanation can be found, this indicates that a risk has been identified. In response, the organisation should review its monitoring.

Electronic video and access monitoring

Video monitoring can prevent fraud. Electronic video surveillance often detects fraud taking place. This is because individuals:

- Forget that it is occurring
- Mistakenly believe that the system is not working or the cameras are looking the other way
- Sometimes do not realise that their activities are on camera
- Sometimes are detected because their whereabouts at a particular time and place can be verified.

Access monitoring keeps track of people as they enter, move around and leave premises. These movements can be analysed. This may help to identify suspects who accessed important areas.

Where analysis of video or access monitoring records gives rise to concerns these should be fully assessed and managed as appropriate.

Where evidence of possible fraud emerges (as distinct from evidence of a risk) then the agency or council should investigate.

Agencies and councils must ensure that they comply with the *Workplace Video Surveillance Act 1999*. This Act provides that video surveillance can only be undertaken with the knowledge of employees, using visible cameras and using signs to warn employees. Covert surveillance cannot be undertaken without an authority issued by a Magistrate.

Risky third party transactions

Organisations should closely monitor transactions involving third parties that may pose significant risks. Third parties can have attributes that should be “red flags” to agencies and councils. Some examples are:

- Poor fraud control. A third party that does not have appropriate fraud control measures is a potential risk to a customer agency or council.
- Errors. Suppliers that make numerous errors may inadvertently cause loss. They may be using the errors to hide fraud
- Established relationships. Long-established suppliers may use a customer’s trust to commit fraud
- Marginal suppliers. Organisations can become involved with financially weak suppliers. There is a risk that the supplier will try to overcome its difficulties by defrauding its customers
- Paperwork problems. Detection of fraud is difficult if records are incomplete or inaccurate. Reconciliation of transactions can be delayed. Losses can mount. Trails go cold and evidence disappears. This may be a deliberate attempt to conceal fraud
- Sole client. An organisation is the sole user of a supplier’s goods or services. Unhappiness, personal problems or a contract about to finish might all lead to such a supplier resorting to fraud.

What do we suggest that agencies and councils should do?

- Ensure that all transactions are accurately captured and reconciled
- Ensure that the level of fraud risk determines transaction monitoring activities
- Ensure that all transactions are subjected to verification to protect the organisation from practices such as skimming
- Establish an internal audit regime that regularly checks sufficient samples of transactions
- Conduct frequent un-programmed spot-checks of transactions both internally and externally
- Actively promote the reporting of suspect, unusual or irregular transactions
- Design systems that actively involve customers in transaction monitoring

-
- Encourage customers to complain where a transaction has not been properly conducted
 - Ensure that all transaction information is assessed for fraud risk implications
 - Ensure all information received (including complaints) is assessed for risk indicators
 - Carry out electronic monitoring of premises, staff and transactions
 - Establish systems for the close monitoring of transactions with and by third parties generally
 - Establish systems for higher level monitoring of transactions with high risk third parties.

What are your ideas and perspectives?

Do you think the features listed here are important in fraud prevention?

Do you have any more suggestions for transaction monitoring?

Do you think describing the activities of agencies and councils in terms of transactions is appropriate?

How should organisations investigate fraud?

How we see it

The purpose of a fraud investigation is to find out as much as possible about what happened. It is not to establish the guilt of a suspect. All evidence uncovered must be available for considerations by the investigators and later.

Most investigative and law enforcement agencies conduct fraud investigations using multidisciplinary teams. These teams usually consist of experienced investigators, lawyers, analysts, computer forensic specialists, accountants and other specialists. This is because of the growing complexity of investigations.

From time to time all public sector organisations have to conduct an internal investigation or commission one from outside. We hope this section is a useful resource when they do.

A risk management committee should provide management input and consider reports during an investigation. It should be responsible for the final reports and recommendations to management.

If you need any further help or advice about conducting an internal fraud investigation see the list of readings at the end of this publication.

Confidentiality first

Whenever an allegation or suspicion of fraud arises the first thing to do is to ensure confidentiality. This is because by releasing information there can be serious damage to the investigation and to the suspected fraudster. The suspected fraudster could:

- Be innocent
- Destroy documents
- Wipe computer records
- Replace goods or money
- Co-ordinate stories with others
- Concoct alibis
- Threaten witnesses
- Sabotage the organisation
- Arrange to implicate others
- Disappear.

An investigation takes time to complete. It is important to keep things confidential for as long as possible. People should only find out about the investigation when it is necessary.

There are other risks if confidentiality is not observed. Unnecessarily revealing that people have provided information can cause embarrassment and damage to the reputations of those involved. It

can also cause gossip to spread throughout an organisation. Potential witnesses may feel that they cannot trust the investigators and not come forward with relevant information.

Need to know

A “need to know” principal should determine what information is made available from the initial disclosure to the final outcome. This reduces the risk that evidence will be lost or destroyed, and helps protect both the complainant and the subject of the investigation.

The longer confidentiality is maintained the more likely it is that an investigation will uncover what happened.

Objectivity and impartiality

At the outset of any investigation you must ensure that the investigators and those they report to have no conflicts of interests. Conflicts of interests can prevent the investigation from being done properly. They can also make it appear that it was unfair to the suspect, did not look for all the evidence, or considered irrelevant material.

Conflicts of interests can arise because of:

- Personal relationships with suspects, informants or witnesses
- Financial relationships with suspects, informants or witnesses
- The possibility of benefiting or suffering because of an outcome
- Personal or professional bias (real or perceived).

Assessing information

All information received relating to possible fraud needs to be assessed to check that it is genuine. This means checking if fraud is likely to have occurred. Next you need to decide whether the matter should be investigated internally or reported to someone else.

Assessment is an ongoing process throughout an internal investigation. New information or a different view of existing information can mean that decisions need to be reviewed and different directions followed.

Investigators have an important role to play at each stage of this assessment process. A major factor in the success of an investigation is how well the investigator records and communicates information. Those who need to be kept informed include people with specialist knowledge, management and others who have a role in assessment decisions.

Some of the issues to be considered are:

- How much specific evidence is there to support the information provided
- Is the information trivial, frivolous or vexatious
- How long ago did the alleged misconduct occur

-
- What resources are available to investigate the allegation
 - How much evidence is there to support the information provided?

The more specific the allegation and the more evidence there is to support it, the more likely it is that it will need to be investigated.

Sometimes the information may be no more than someone's suspicions about what might have occurred or be occurring. In such cases you need to consider:

- The nature and impact of the fraud if the allegations are true
- Whether there have been similar reports
- Whether it could be connected with some other fraud suspicion or allegation
- Whether different allegations have been received about the same employee or section.

Trivial, frivolous or vexatious

Some allegations are so trivial or insignificant that they need not be investigated. These allegations can arise from personal animosities or other motives that have nothing to do with the existence of fraud.

But a matter cannot be ignored just because the source of the information might have questionable motives.

Investigators have to be more cautious about accepting the accuracy of the information supplied. In these circumstances it is important to find independent evidence that supports the information.

Age of alleged fraud

An allegation might involve a fraud that occurred so long ago that it is impossible to justify an investigation. This is because:

- Witnesses may be difficult to locate
- Memories of the circumstances have faded
- Documents have been destroyed or lost
- Offences committed long ago are more lightly punished if proven
- It is unlikely that any losses will be recovered
- It is unlikely that any prevention lessons will be learned.

The less serious the matter and the older it is, the more likely it is that it should be dismissed at the assessment stage.

Impact

You need to consider what impact an investigation will have on the organisation. This will depend on a number of factors. It is important to consider the impact on:

-
- Resources of the organisation
 - Morale of staff
 - Perceptions by staff of attitudes to fraud and ethics generally
 - The level of risk of fraud being perpetrated again
 - Capacity to fully identify the level of damage done.

Reporting the matter to the ICAC

All NSW state agencies and councils have a duty to report any suspected corrupt conduct to the ICAC. Corrupt conduct is defined in sections 8 and 9 of the *Independent Commission Against Corruption Act 1988*. Fraud is included in that definition.

Fraud should be reported whether or not it is perpetrated by a public official. This is because all fraud impacts in some way on the ability of public officials to do their jobs effectively.

When a matter has been reported to the ICAC, the ICAC may ask the agency to arrange for it to be investigated. In this case you have a choice of doing it in-house or engaging an outside investigator.

The ICAC might decide to investigate the matter itself. It would decide on the basis of how it sees the particular case impacting on the public sector generally. For example, the ICAC would probably look at a new type of fraud involving major losses. This would be because lessons applicable to the whole private sector might emerge.

The ICAC Act requires all agency heads and council general managers to:

“... report to the Commission any matter that the officer suspects on reasonable grounds concerns or may concern corrupt conduct.”

This means that you must report to the ICAC as soon as you suspect fraud. You must not wait until an investigation is underway. This is because the ICAC might want to investigate the matter confidentially.

What do we mean by “suspects on reasonable grounds”? It means there must be a real possibility of corrupt conduct. Certainty is not required. You may not have any clear proof, or even an identified suspect. But these matters should still be reported. The real question is whether the conduct gives rise to a suspicion of corruption. If you are not sure, call us and discuss it.

Who should carry out a fraud investigation

If you decide that a matter should be investigated, the next issue is who is going to conduct it.

There are a few options:

- Conducting the investigation internally using your organisation’s own resources and skills
- Arranging for the investigation to be conducted by an outside agency or service provider.
- If the losses are insured against (particularly worker’s compensation claims and other insured risks) handing the matter to your organisation’s insurer to investigate.

There are a number of issues to consider in deciding if you are going to conduct the investigation. You need to decide if you have the people and resources to investigate the matter. You will need to have available at least some of the following:

- Investigators who are not involved in the fraud and have no conflicts of interests
- Access to sufficient skills in evidence collection, preservation and presentation
- Access to skills necessary to conduct and properly record interviews
- Access to skills necessary to prepare in house reports and disciplinary papers.

A multi-skilled team will often be required to investigate fraud. The degree of expertise will determine if you need to hire specialists or to rely on in-house knowledge. You will need access to knowledge in areas including:

- Legal, disciplinary and industrial procedures
- Accounting
- Computing
- Procurement and disposal procedures and practices
- Transaction tracking and reconstruction.

Either at the beginning or later, you may need to be able to access skills necessary to prepare briefs to counsel or prosecution briefs for Police and the DPP.

If your organisation has these skills available you should be able to conduct an investigation into an alleged fraud. Remember though that at various points during an investigation you may need to review this decision. The steps to follow in an investigation are set out later on in this paper.

Outsourcing

If you have doubts about the ability of your organisation to investigate an allegation of fraud you should seek help. A number of options exist including:

- Seeking the assistance of the Police or other investigation agencies
- Develop a shared investigation capacity with another like agency (e.g. neighbouring council)
- Hiring an outside adviser to assist internal investigators
- Commissioning an outside investigation.

When a matter is reported to the ICAC it might decide to investigate it. Or it might ask an agency to conduct or arrange an investigation. You can contact the ICAC if you need advice on how to go about investigating a suspected fraud.

A number of legal and accounting firms conduct fraud investigations. A number of investigation specialists such as private inquiry agents do the same. You may need to consider using one if you have any doubt that you have the skills and resources to conduct an investigation.

The NSW Police and the Association of Certified Fraud Examiners are developing a Memorandum of Understanding. The MOU will deal with collaboration between Police and private investigation

specialists. This may allow for resource sharing. This might mean that services like forensic accounting, computer forensics and intelligence are undertaken by private investigators rather than the Police. This model shows that agencies and councils need not take an 'all or nothing' decision on whether to outsource the investigation. Some issues can be handled externally, while others can be done in-house.

The aim is to strike the right balance. Here are some factors to consider:

- The cost of using specialist investigators
The cost of outside help should be viewed in the context of the damage that continuing, or unexposed, fraud could do to your organisation.
- Your insurers requirements
Your insurer will be interested in ensuring that the matter is properly investigated. This is because they will want to make sure that future loss is minimised.
- The expertise available in-house
You need to consider the strength of your in-house expertise. It may mean you take the matter as far as your own expertise will allow and then seek help. It may be that you need someone from inside who understands your organisation more than you need a specialist investigator.
- Technological aids that may be needed (such as computer forensics, forensic auditing and video surveillance)
This kind of specialist assistance is rarely available in-house. You may also need help with the legal issues arising from this kind of evidence gathering. Again, though, you may only need this sort of outside assistance, but continue to manage the bulk of the investigation in-house.
- Whether you will need coercive powers such as search warrants
If the investigation cannot proceed without coercive powers, then the matter should be handed over to the Police.
- Conflicts of interest and probity
Fraud investigations are often difficult times for agencies. But this doesn't mean that the essential elements of good contracting practice can be ignored.

These decisions must be taken with attention to the primary considerations of serving the public interest and meeting community expectations.

You cannot outsource the job of monitoring the progress of an investigation. If an outside organisation is to conduct any part of investigation you still need to nominate someone to:

- Liaise with the investigators
- Arrange resources
- Introduce investigators to people
- Report to responsible management
- Provide relevant operational knowledge and experience.

Planning an internal investigation

Good planning and preparation are important factors in the success of any investigation. As soon as you have decided to conduct an internal investigation, you need to find the right people, establish an investigation file and prepare a formal investigation plan. You should start keeping a diary or notebook to record details of your part in the investigation.

Investigation file

An investigation is the process of uncovering and recording evidence. That evidence, and the way it was obtained, must be presented in a manner that is acceptable in subsequent proceedings. It must be possible to trace the investigation from start to finish. It must also be possible to identify where evidence came from and how and when it was obtained.

For these reasons it is necessary to establish a confidential investigations file. This file should be accessible on a strictly “need to know” basis.

The file and its contents may be subpoenaed in civil or criminal proceedings. The file may also be used in disciplinary proceedings. It is important therefore that it is kept secure and maintained in an orderly fashion.

This file should contain all material about the investigation, including:

- The original allegation
- Any evidence collected during initial inquiries.

The information should be:

- In chronological order
- On a dated index or running sheet for all new material added
- Accurate and reliable
- In compliance with procedures for protecting confidential information.

You need to keep file notes of the content, dates and times of:

- Discussions
- Phone calls
- Interviews
- Information or evidence received from witnesses or other organisations
- Reports provided by experts
- Witness statements
- Transcripts of records of interviews
- Progress reports
- The final investigation report.

Note that only copies of evidence should be kept on this file. Original witness statements and exhibits should not be kept on this file. There is a risk that they will be marked, lost or stolen. Original documents and exhibits should be kept in a secure locked safe or cabinet.

Good record keeping is essential in all investigations. It helps you to see links between various pieces of information and to keep track of where the investigation is going. It also makes later tasks, such as writing reports and preparing briefs of evidence, much easier.

Formal investigation plan

A proper fraud investigation needs to be planned. The plan identifies what you are trying to do and how you intend to do it. It also identifies who will help you and in what way.

The investigation plan should establish the focus and limits of the investigation and help you to organise, manage and review the investigation process.

It is important to start with a plan. But you must be prepared to revise it during the course of the investigation. You also need to consider practical issues such as the availability of resources. Where necessary, responsible management must approve the investigation plan before the investigation starts.

If the investigation is being conducted internally, it is a good idea to discuss the available facts with a more experienced investigator. For example, you could ask the Police, the ICAC, the NSW Ombudsman or the Department of Local Government for advice.

The plan should include:

- A description of the alleged fraud
- The objectives of the investigation
- The scope of the investigation and the strategies to be used
- Details of any initial inquiries
- The resources needed
- The time frame
- Review points and times
- Finalisation arrangements.

A description of the alleged fraud

You need an accurate description of the alleged fraud. This will be broken down into its elements if possible. These would include such things as the:

- Nature of the allegation
- Possible criminal offences
- Proofs necessary to establish the offences
- Possible disciplinary offences
- Relevant sections of the *Public Sector Management Act 1988*
- Relevant sections of staff awards
- Relevant sections of a code of conduct.

Objectives of the investigation

These are often to identify:

- Alleged wrongdoer, if not already known
- Facts which need to be established in order to prove (or disprove) the allegation
- Means by which those facts can be established
- Evidence required to establish the allegation and the means of collecting it in legally admissible forms
- Need for changes to systems, personnel, policies and procedures.

The scope of the investigation

It is usual to set limits to the range of the investigation and on how long it will be allowed to take. For example, you might decide to limit the investigation by looking for evidence of what happened only in the previous twelve months. Or you might decide to limit it to spending twenty hours of effort on the case before reviewing your involvement.

You might wish to keep the investigation confidential until you have interviewed witnesses. Or you may feel confident that you have accurately identified the alleged wrongdoing and have sufficient evidence or information available for you to confront the subject person with the allegations.

Methodology

This involves identifying how and when you will:

- Obtain additional documents, files and computer records
- Obtain additional information
- Obtain corroboration of what you already have
- Interview possible witnesses
- Confront the alleged perpetrator
- Report to responsible management
- Involve outside authority.

Details of any initial inquiries

Care must be taken to accurately and objectively record the results of preliminary inquiries. At various stages, this information will be central to the decision of whether or not to investigate the matter further

The details you need will usually include:

- Results of preliminary inquiries
- The source of the information
- An assessment of the reliability or accuracy of the information (possibly using a system of ratings ranging from highly reliable to highly doubtful)
- Details of different sources that appear to confirm the same facts (corroboration).

The resources needed

You need to ensure that you have access to resources such as:

- Internal personnel
- Equipment
- Travel
- External advice if required
- Additional skills or expertise.

Time frame

The time frame of an investigation will depend of a number of factors including:

- Statutory bars (e.g. where charges must be laid within a certain time)
- Witness availability (e.g. about to go overseas)
- Resource limitations
- Age of alleged fraud.

Review points and times

Review points and times need to be set to ensure timely:

- Assessment of progress against plans
- Review decision to investigate internally (where necessary)
- Confirmation or amendment of strategy
- Completion of stages and tasks
- Consideration of results so far
- Amendment of timetable where evidence warrants.

Finalisation arrangements

You need to decide who will do what at the end of the investigation.

You need to include a timetable and decide who will be responsible for:

- Writing the final report
- Developing recommendations for legal or other proceedings
- Approving legal or other proceedings
- Preparing briefs of evidence
- Authorising other follow-up actions
- Implementing administrative changes
- Continuing custody and eventual return of property and other evidence
- General administrative finalisation of the matter.

You may come across interesting “off-shoots” that could indicate wider misconduct or your inquiries may uncover other offences. If this happens and you decide these offshoots are important, they need to become part of a new and separate assessment and investigation.

Reconstructing transactions

Where a fraud is suspected you usually need to reconstruct how it was done. You can do this by adapting the measures for monitoring transaction referred to earlier in this paper. Instead of being used to prevent fraud, these measures are used to build a picture of what has happened.

Reconstruction means putting yourself in a position to describe the fraud. It involves finding out how, where and when the various parts of the fraud were conducted. It is the often laborious task of putting together the paper or electronic trail showing where the money went and why. You can get information from:

- Accounting information. Verification records such as receipts, cheque butts, bank statements and computer records can help you follow the money trail.
- Performance assurance. Records of payments and apparent proofs of expenditure can be checked. They may have been falsified in order to cover up the suspected fraud
- Internal audit records. Where these appear to be in order it is necessary to identify whether the audit was misled and the results of a fraud were hidden.
- Internal reporting records. It may be that previous reports that have been dismissed might be of relevance in the light of information being unearthed in a wider investigation
- Customers. Interviews with customers might uncover transactions that did not take place, were not recorded or were conducted improperly.
- Reconciliation of information. Fraudulent transactions will often appear to have been properly reconciled. Records should be re-checked to find the items have been falsified.
- Electronic monitoring records. These can be useful to establish who had access to relevant places or records and at what times. They should also reveal what was done with or to the data involved.
- Risky party transactions. The results of the closer monitoring of risky parties can be very useful in reconstructing transactions. They should allow you to identify each aspect of the transactions and build up a picture of what happened.

The records and data used to reconstruct transactions must be handled with great care. It may be needed to prove the reconstruction. Original records should be kept in a safe place. See the section on handling of evidence in this paper.

It is important to bear in mind the continuing need for confidentiality in fraud investigations. This is because a proactive, or covert, phase might follow the reconstruction. For example, you might decide to allow a fraud to continue so that you can better understand its full extent. You might also want to take time to identify other perpetrators. If an external agency is to conduct the investigation it too might wish to keep the matter confidential for a time.

Collecting and handling evidence

All investigators must ensure that evidence is collected and handled scrupulously. This is because any doubts about the admissibility of evidence can lead to the failure of proceedings. This might lead to the failure of a prosecution, disciplinary case, unfair dismissal defence or attempt to retrieve the proceeds of a fraud.

If evidence is obtained in the wrong way it may be inadmissible. It might also be inadmissible if it is kept or transferred from one person or place to another incorrectly. In such circumstances it is no longer possible for an investigation to achieve much of its objective.

Investigators may need to obtain items or documents, such as files or invoices, from the original information provider or from other employees within the area or section involved. Most frauds will involve the use of documents to deceive a public official. On other occasions attendance records, delivery details or expenditure dockets will be used in fraud.

Searching

Evidence of fraud can be found in many places. It is important that it is found lawfully and in a way that allows evidence to be used. Sometimes this is a problem. For example, it might be necessary to search personal property such as bags or cars.

Investigators cannot enter or search private property, such as a person's home, car, briefcase or wallet, without permission unless they have a search warrant. Internal and private investigators are not able to get search warrants.

Any evidence gathered illegally is not likely to be admissible. Anyone who searches private property without a warrant or permission is committing an offence.

With permission from senior management of agencies or councils, investigators are allowed to search a suspect's office or workplace. It is always better to have evidence and not need it than to need the evidence later and not have it.

You should look for anything that might be relevant to the fraud investigation, such as:

- Documents, notes, yellow stickers, or messages
- Official diaries, notes and receipts
- Waste paper bin contents
- Teledexes
- Answering machine records
- Impressions on writing pads and blotters
- Samples of the suspect's handwriting
- Computers, computer disks and other data storage (including Internet and email logs).

Evidence on electronic databases

Computers often contain information vital to a fraud investigation. It is important to keep computer records in the state in which they were found. When gathering evidence, if computers are switched on in the wrong way valuable evidence can be lost or contaminated. The normal way of starting a computer will cause such losses.

Specialist investigators obtain information from computers by mirroring the computer. Data can be lost if the machines are not turned on properly.

Do not allow anyone to turn on a computer that is used by a fraud suspect unless they are fully trained and equipped to do so properly. Make sure to arrange for the preservation of records stored centrally. These might be on a shared or local area network.

Computer data can also be stored on peripherals including floppy discs, portable hard drives and central backup logs. Attempts should be made to locate and secure any of these. Remote email addresses should be recorded for possible later checks. The accounts should not be accessed without permission or a warrant.

Individual logins and passwords control and record various accesses. Improper accessing of data is a prime fraud technique. Access records should be located and secured. These might provide valuable data about who did what, where and when.

There are dangers when it comes to voice mail and other telecommunications. Even when recorded, listening to these can be a crime under Commonwealth or NSW legislation.

Suspects' presence at searches

It is not necessary for suspects to be present during a search in the workplace. However you might decide to arrange for them to be there. You may be unable to prevent them from being present.

If present, the suspect might threaten the investigation by attempting to remove, destroy or otherwise compromise evidence. You should be prepared for this. You should never conduct a search alone.

Steps you should take include:

- Ensuring that an independent person is present
- Considering video recording the search (do not record speech without permission)
- Considering photographing the scene and evidence gathered
- Recording time and date of search as it happens
- Recording where and when items are located as they are found.

The witness to the search should also be available to complete statements if that becomes necessary later on. The witness should countersign records of the search.

It is important that records, such as official diaries, notes or receipts, are not removed or destroyed by the suspect or another member of staff either deliberately or by mistake.

Experts

You may also have to collect information from a range of “experts”. For example:

- Forensic accountants may reconstruct suspect transactions
- Doctors may provide medical details concerning a persons claims
- Auditors may analyse financial systems or help follow a money trail
- Computer experts may be able to help with information technology issues.

Examination of evidence

If you need documents examined, especially for fingerprints or other evidence of handling, make sure you:

- Do not fold, staple or perforate them
- Do not continually handle them
- Put them in seal-able bags or envelopes with an identifying label on the bag not on the document
- Do not use plastic bags because they sweat and may damage the documents
- Take photocopies of the documents to use as working copies.

Handling evidence

All evidence must be kept in a secure place. It might be inadmissible if it is kept or transferred from one person or place to another incorrectly. In such circumstances it is no longer possible for an investigation to achieve much of its objective.

The more contentious the evidence or the more susceptible it is to being damaged, altered or confused with another similar exhibit, the greater the need for security and continuity of control.

For example, it may be acceptable to send a document for expert examination of the typeface or handwriting by registered post. This can only be done when a witness can readily identify it and the document is not central to the whole investigation.

However, if you were sending physical evidence to laboratory for analysis to a, you would need to be able to prove a continuing chain of possession and control from the time the sample was taken to the time it was analysed. This would apply to documents being examined for fingerprints or other evidence of handling.

As a general rule, it is preferable not to trust important exhibits to the postal system or couriers.

Transferring evidence

As the investigator, you are responsible for recording the receipt and hand-over of any property or evidence on some form of register, and making sure that a chain of evidence is maintained. You must be able to trace the origin of a document or item and the various processes or people it has passed

through. Otherwise the document or item may end up being inadmissible as evidence. All documents must be kept in their original condition, unless they have to be altered during forensic examination.

Some of the precautions you should take are:

- Always issue a receipt for property that is received or seized
- Make sure original documents or items are not marked, changed, lost or damaged in any way
- Avoid handling critical documents, especially if a police investigation is likely
- Keep records of where, when and by whom the evidence was collected and fully describe each item or document on an exhibit register
- Store items in a secure area, for example a safe or strong room. Investigators may take items such as files or tapes out of storage to work on in the office, but the items must never be left lying around or unattended.

Copying evidence

Photocopying of documents requires particular care in order to ensure that the handling trail is not broken and the evidence put in doubt. The kinds of items that you might photocopy include documents, photographs and cheques. Take photocopies of documents and photographs of items such as cheques that may be used as evidence.

Precautions include:

- Record who did the copying and make sure they check the copy against the original
- If files are seized as evidence and it is necessary to make working photocopies, it is essential that the original order of the contents of the file not be disturbed
- In some cases, it may be better that you do the photocopying rather than entrust it to someone else who may be less sensitive to the needs of the investigation
- Try to minimise the number of people who might mishandle the evidence and so complicate things if there is a dispute.

Interviewing witnesses

Investigators interview people to find out what they know about an incident or other circumstances surrounding a fraud. It is important that interviews are carried out properly so that:

- All knowledge relevant to the fraud is revealed
- The information is admissible in evidence
- Nothing is overlooked (you may not get a second change to ask questions).

During an investigation you are likely to have to interview employees of the organisation or members of the public. You are also likely to need to interview alleged perpetrators.

If you are interviewing a person under the age of eighteen, you should ensure that a supportive adult is present. This may be their parent, friend or lawyer.

It is important that all interviews be conducted properly. There are a number of things that an investigator should bear in mind during investigative interviews.

Location

You need to consider when and where the interview will be held and what equipment and documents you may need. You need to ensure:

- The location is private, quiet and comfortable, and free from the possibility of interruptions and distractions
- There are toilet facilities and refreshments available
- The person being interviewed is comfortable.

Time

If the interview is going to be held during office hours, it should cause as few disruptions as possible to the work of the organisation.

Interviews held during work time have advantages including:

- That staff feel obliged to co-operate
- Human resources staff and union representatives are more likely to be available
- It is easier to verify work-related matters that may come up in the course of the interview
- If an employee refuses to answer questions in a workplace interview this may be a disciplinary matter.

Presence of others

Whether you are interviewing a witness or a suspect, you should do so in the company of another person. That person should:

- Be familiar with the investigation so that he or she is able to assist with the questioning
- Take notes
- Be able and available to corroborate what was said during the interview.

Persons being interviewed should have the option of inviting another person. This person:

- May be a union representative, solicitor or colleague
- May only adopt a supportive role
- Is not there to tell the witness what evidence to give or to take over the interview.

Note: If it becomes impossible for the interview to be properly conducted, it should be ended and new arrangements made.

Equipment

You should make sure that you have everything on hand that you might need, including:

- Note paper and writing implements
- Video recorder
- Tape recorder
- Computer
- Forms, diagrams, photographs
- Documents and other items of evidence
- TV monitor.

When

Your first witness interview is usually when you take a statement from the complainant as part of your initial inquiries. You then need to decide the order in which you interview the remaining witnesses. This will depend on:

- The importance of their evidence
- Their degree of association with the suspect
- The need to conduct the interview while facts are still fresh in their minds.

Statements

Formal statements are designed so that they can be used as evidence in a court of law. A witness statement should accurately reflect what the person being interviewed wants to say. Formal statements involve the person being interviewed agreeing to sign-off on what they have said.

In some cases a court may not allow evidence additional to the statement to be given. It is therefore essential that all relevant evidence is included in the statement.

Formal statements have other benefits including that they can:

- Reduce or eliminate the number of times the witness is required to attend court to give oral evidence in the witness box
- Help witnesses at a later date to refresh their memory about a particular matter
- Provide information for management to help them make decisions about how to deal with the complaint
- Be used by police, prosecutors or other investigators
- Be used by the suspected person or his or her legal representatives.

Taking a statement

Before you start taking the statement, ask the witness to tell the story from beginning to end in his or her own words. Their statement should then follow the same chronological sequence of events.

In civil proceedings the evidence is usually contained in a sworn affidavit. The rules of the court and the laws of evidence govern the form and content of affidavits.

In criminal proceedings for more serious crimes (known as indictable offences), the form of the statement is governed by the *Justices Act 1902*. The police and most investigators use this format. It is a useful one to adopt, even if the matter under investigation is not a criminal one. This form impresses upon the witness the importance of the occasion.

Form of the statement

The first paragraph of a statement under the *Justices Act 1902* must, subject to a few exceptions, be in the following form:

This statement made by me accurately sets out the evidence which I would be prepared, if necessary, to give in Court as a witness. The statement is true to the best of my knowledge and belief, and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it anything that I know to be false or do not believe to be true.

You must ensure that:

- The witness signs every page of the statement
- The witness initials any corrections made
- You counter sign the witness's signature on every page
- You countersign all initialled amendments
- All pages are numbered (e.g. page 1 of 6 pages)
- The statement is dated
- There is no blank space left between the end of the statement and the signature
- The witness's date of birth or age is included.

Laws of evidence

The laws of evidence make provision for the type of evidence that a witness can give in court and the way in which it can be given.

When taking a statement from a witness, you should try to comply with those laws so that inadmissible material is not included in the statement.

As already indicated, the strict laws of evidence do not bind some tribunals so that the form and content of the statement may not be so critical. As a guide, the more serious the matter you are investigating, the more formal the statement will need to be.

The following paragraphs describe some of the issues that can arise in statements. Many also arise when people are giving oral evidence. What follows is a brief overview. If you are unsure about these aspects you should seek legal advice.

Hearsay

Hearsay is what someone else has been heard to say about an event. The fact that the person made such a statement is not admissible in evidence if the purpose of the evidence is to prove that the event heard spoken of occurred. For example it would not be acceptable for Jim to say that he heard John say that Bill admitted to a fraud.

As a general rule hearsay is not admissible as evidence in criminal proceedings. It may be admissible in ICAC, Ombudsman or disciplinary hearings.

Opinion

As a general rule, a witness should not include expressions of opinion about something or someone in his or her statement. That is unless the witness is an expert who is required to provide an expert opinion on an issue.

Annexures to statements

Frauds usually involve the use of documents. These are sometimes referred to in statements. When they are you should include copies of any documents or things referred to in the statement. These are annexures.

The annexures should be referred to in a statement like this:

I have been shown a copy of document marked annexure '...' I recognise that document as a copy of the one that I saw Roy take from Tony's desk.

A copy of the annexure should be clearly marked, usually at the top of the page, "Annexure ...". Never mark the original document.

Sometimes a witness may have made contemporaneous notes of a fraud related incident. That is, one made at the time or shortly after. If those notes are referred to in the statement, a copy of them should be made an annexure.

Interpreters

If the witness speaks little or no English, or is deaf, then the statement should be taken using an interpreter.

The Community Relations Commission of NSW can provide suitably qualified interpreters. Except in cases of emergency, you should not ask a relation or friend of the witness to interpret

You will need to take a statement from the interpreter stating his or her qualifications and reciting the fact that they prepared an English translation of the witness's statement. A copy of the witness's original statement and the certified translation should be annexed to the interpreter's statement.

Telephone statements

Try not to take formal statements from witnesses over the telephone. You should only do this if the statement is needed urgently and the witness is located far away.

It is difficult for you to make an accurate assessment of the witness over the telephone and mistakes in the statement are more likely to occur.

If at all possible, fax or email a copy of the statement to the witness to approve or amend and approve. The approved statement should then be signed and faxed back to you with the original to follow.

Unsigned statements

Sometimes an employee or member of the public is prepared to speak to you about a matter, but is not willing to provide a formal statement or record of interview. You should take detailed notes for future reference. If the person agrees, ask them to sign the notes to acknowledge that they are accurate. Try to write the notes while you are speaking to the person or as soon as possible afterwards.

The purpose of taking the notes is to assist the person who is calling the witness to anticipate what evidence the witness might give. Ensure that you:

- Include the date and time of the conversation
- Include the date and time that the notes were written up
- Keep them on file in a safe place.

One reason why a complainant may be reluctant to talk to you or provide a signed statement is that he or she fears reprisal for making the disclosure. If this is the case, and the person is a public official, you should advise them of the provisions of the Protected Disclosure Act.

Interviewing suspects

A suspect must not be formally interviewed by anyone who is not qualified to conduct the interview.

It is most important that any interview with a person suspected of fraud is conducted properly. If it is not, any chance of a conviction being obtained, or even of them being dealt with by disciplinary means, might be lost.

Timing

Unless there are compelling reasons for doing so, do not interview a suspect until you have collected and assessed all the available evidence.

Make sure you:

- Set objectives for the interview
- Prepare a list of essential issues to be covered
- Familiarise yourself with all the facts and details of the case.

The more serious the matter, the more formal the interview is likely to be.

Preparation

If you need to show documents or other things to the suspect make sure that you have them ready and available. If there are a lot of documents, you should consider the order in which you intend to show them to the suspect. Place them in a file in that order.

If you are working with another investigator, make sure you decide on your respective roles before you start the interview. For example, who is going to ask which questions and who is going to take notes, produce the documents and such.

Suspects' responses

Think about the suspect, his or her background, any possible responses, defences or alibis and how they are likely to react during the interview. Be prepared for a suspect to:

- Stay silent
- Refuse to answer certain questions
- Lie
- Be anxious
- Be aggressive
- Never stop talking.

Confidentiality

It is important to consider the needs and welfare of the suspect as well as the need to make progress with the investigation.

- You should be discreet about the fact that you are interviewing the person as a suspect
- The interview should take place in suitable surroundings where you are assured of not being interrupted
- Arrangements should be made so that the suspect does not have to explain his or her whereabouts to colleagues
- The interview should not take place in view of the suspect's colleagues
- Refreshment and toilet facilities should be readily available.

Interpreters

If the suspect is from a non-English speaking background you should establish whether an interpreter is going to be required. See above for information about interpreters.

Recording

Decide on the way in which the content of the interview is to be recorded. There are a number of options that include:

-
- Video recording
 - Tape recording
 - Typing or handwriting the questions and answers
 - Having a stenographer record the interview.

There are clear advantages in having the interview audio taped or video recorded including:

- The interview flows better
- Fewer notes need to be taken during the interview
- The responses and attitude of the suspect are captured more accurately
- Reduced risk of unfounded allegations of improper conduct being made.

There are some things that you need to bear in mind when conducting recorded interviews:

- Recording will highlight any mistakes you make
- You need to make sure you are properly prepared for the interview
- Still take some notes to help you develop your line of questioning
- To avoid later confusion, make sure that you fully identify any document or other thing shown to a suspect during an interview
- The purpose of recording is always to fully and fairly record the whole of the interview.

Conducting the interview

The purpose of the interview with the suspect is to accurately put the allegation to the person and allow them the opportunity to respond.

This may involve putting details of the allegation directly to the suspect and seeking a response. It may involve asking the suspect to comment upon certain factual matters uncovered during your investigation. For example, you might ask the suspect to explain a discrepancy between a bank statement and a record in an accounts book or you might put it directly to them that it is evidence of fraud.

Behaviour

It is important that you keep focussed on the purpose of the interview. Some things to bear in mind are:

- You must remain calm, polite and maintain objectivity
- You must not allow insults or other attempts to upset you or affect your objectivity.
- To react to provocation leads to loss of focus and purpose
- To react to provocation may mean that some or all of the interview becomes inadmissible.

Ultimately, if the suspect's behaviour is objectionable and no purpose is being served by the interview, you should terminate it, giving the reasons for doing so.

Questioning

Be careful about the types of questions you ask. Remember that, while probing questions are acceptable, questions are not acceptable if they are:

-
- Ambiguous. Capable of having more than one meaning
 - Convoluted. Contain more than one idea or meaning
 - Judgemental. Imply wrongdoing in the question
 - Leading. Taking people to an answer they might not have meant to give (typically closed questions – capable only of a yes or no answer)
 - Deceptive. Implying something is established when it is not.

Your role is not to cross-examine the suspect to bring about a confession or admission. However, if the person chooses to make an admission you should explore the extent of the admission by putting the specific issues for them to comment upon.

A person may be prepared to admit to wrongdoing, but still dispute some of the allegations or the details of the wrongdoing.

As your role is not to cross examine the suspect, you should try and avoid repeating a question unless it is for the purpose of clarification. There is no problem with asking the suspect to clarify or expand on answers, providing it is not repeatedly done so as to intimidate or harass the person.

Don't make any threats or promises, and don't prompt the suspect other than to clarify their answer. If pressure is used or inducements are offered to encourage a suspect to give answers, a court or tribunal will exclude the whole or part of the interview.

Voluntary answers

The suspect's answers must be provided voluntarily. If the suspect does refuse to answer any further questions, terminate the interview immediately and make notes of everything said up to that point. Ask them if they want to make a statement about the matter or add anything to what they have already said.

If during the interview, the suspect indicates that he or she is tired or wishes take a break then that should occur. The time the interview is halted and resumed and the reason for it should also be noted on the record.

Generally, it is better not to discuss the subject matter of the interview with the suspect during the break. When resuming the interview, the suspect should be asked to confirm the fact of the break. They should also be asked what, if anything, was said by you to him or her relevant to the investigation.

Interview structure

An interview is a fact-finding exercise. It needs to be structured properly to ensure that as much useful information as possible is revealed. A useful and commonly used format is:

- The introduction
- The caution, (if applicable)
- A 'do you agree?' component
- A 'what happened?' component
- Specific questions

-
- Closing the interview
 - Adoption of the interview.

The introduction

This is important to set the scene and ensure that no doubts arise later about the circumstances. It should include:

- The time, date and location of the interview
- Details of everyone present at the interview
- Short explanation of how the interview is going to be conducted
- Details of the suspect's full name, date of birth, address and occupation.

The caution

It is not always necessary to caution a suspect at the beginning of an interview. But at some point you may feel that you have enough evidence to prove that a crime has been committed. If that happens you must caution the person being interviewed. If you do not caution at that point the interview might not be admissible.

Cautioning means advising the person that they do not have to say or do anything, but anything that they say or do may be used in evidence.

It is a good idea to have a copy of the following correct wording of the caution with you whenever you are doing an interview.

I want you to understand that you do not have to say or do anything but anything you do say or do may be used in evidence. Do you understand that?

Always make sure that you ask the suspect if they understand the meaning of the caution and repeat it if they do not.

A 'do you agree' component

In this part of the interview you should go back over the events that occurred before the interview. You are trying to obtain the suspect's agreement that this is what actually happened.

A 'what happened' component

Here you ask open-ended questions such as, "What happened then?" "What happened next?" and "Why did you do that?"

Specific questions

You may ask this type of question to clear up ambiguities or to cover elements of the offence or complaint that have not been covered.

Closing the interview

The suspect should be given the opportunity to provide any further information he or she may wish to add, including the provision of a handwritten or typed statement.

Adoption of the interview

Whatever the means of recording the interview, the suspect should be asked to adopt the record of it.

If the interview is being recorded either on video or audiotape, the suspect should be asked, while the tape is running:

- If he or she has any complaints about the way in which the interview has been conducted
- To confirm that answers have been given freely and without any threat, promise or inducement being made to them by anybody.

The outside of the video or audio tape should be labelled with suitable identification including:

- The time and date
- Your signature
- The signature of the suspect.

If the suspect requests a copy of the interview, you should provide a copy as soon as possible, unless there are good reasons for not doing so.

Written records

Where the interview is being manually recorded (handwritten or typed) the suspect should be asked to read the interview aloud. If he or she is unable to do so it should be read for them. It is preferable that someone read it out other than yourself or your colleague.

You should then ask the following series of questions:

- Do you agree you have just read aloud each page of this interview
- Is it a correct record of our interview
- Have the answers you have given as recorded in this interview been made of your own free will
- Has any inducement, threat or promise been held out to you to give the answers that have been recorded in this interview
- Will you read aloud these additional questions and answers (if applicable)
- Will you initial any errors that may appear in this interview
- Will you sign each page of the interview?

Then suspect should:

- Sign every page of the interview
- Initial all corrections.

Then you should:

- Witness all signatures of the suspect
- Initial any corrections endorsed by the suspect
- Provide a copy of the statement to the suspect
- Have the suspect sign for the copy on the original.

Confession statements

Sometimes a person may want to make a confessional statement about a crime. If this happens it is important that they be properly and fully cautioned before they do so. Use the caution quoted above.

Make sure you remain impartial and allow the person to write the statement in his or her own words. Do not put words in their mouth.

You should have the person sign the confession statement and have the signature witnessed.

You should provide the person with a copy of the statement.

Investigation reports

Investigators may have to prepare a variety of reports at different stages of an investigation. The purpose of these reports is to communicate information about the matter being investigated.

Reports will form the basis on which decisions about what happens next will be based. Those decisions might be taken before, during or after the investigation.

There are a number of types of reports. Each is prepared when an investigation has reached a stage or date on which they are required. Depending on the type of report, it should include:

- Date and mode of initial complaint or disclosure
- Details of the allegation
- Initial inquiries made
- Investigation plan (if appropriate)
- Progress report (if appropriate)
- Assessment of the information collected (or collected so far)
- Recommendations about future action
- Name of author
- Date report completed.

Assessment reports

An assessment report is usually prepared after you have made a preliminary assessment of the complaint and completed some initial inquiries. It is written to assist those responsible to consider the matter and decide what action should be taken.

Investigation plan

An investigation plan becomes a report when it is submitted to decision makers for endorsement. We discussed these earlier.

Progress report

Investigators may have to provide decision makers with regular reports on the status and progress of an investigation. The reports are an important accountability and review mechanism. They help decision makers to keep up-to-date with what is and should be happening.

They may be produced to a timetable. Or they may be prepared if the investigation produces significant or unexpected findings. You may also produce a progress report if there are resource problems or you feel that an alternative approach or focus needs to be adopted.

Final report

A final report differs in content from the others. It has additional features as it represents the end of the investigation. It will outline the results of all your inquiries and your recommendations for any:

- Referrals
- Disciplinary action
- Prosecutions
- Corruption prevention steps.

The report should consist of two sections. The first section should cover the facts relating to the investigation. A suggested structure is:

- Covering memo/executive summary
- Background (scope of the investigation, sources of information, methodology)
- Results of inquiries
- Conclusion
- Recommendations (disciplinary action and such).

The second section should cover general issues raised by the investigation. Someone other than the investigator might complete it. It might address:

- Comments on any perceived adverse repercussions for the organisation
- If and why correct procedures were not followed
- The need for new procedures or controls to prevent future problems
- Recommendations for systems improvements.

Summary of evidence

An investigator may also have to prepare a summary or brief of evidence for the Police, a court of law or an industrial tribunal. This is a collection of all the available evidence that may be needed for a disciplinary action or criminal prosecution.

For briefs of evidence, there are some specific requirements that need to be satisfied. The original brief should be kept in a locked and secure environment until prosecutors need it.

You will need to prepare two copies of the original brief for:

- Senior management or the appropriate external agency
- Keeping as your working copy.

If you are not sure what should or should not be included in the brief, make sure you get advice from an experienced investigator or investigative agency. The brief of evidence should include:

- A covering memo/letter to senior management or the external agency
- An index of contents
- A copy of the final investigation report or an executive summary of this report
- Documents such as witness and property lists
- Signed witness statements and copies of annexures referred to in the statement
- Signed records of interview
- Other relevant evidence such as printouts, extracts of policies and microfilm records.

Often, a summary of evidence is sufficient. The NSW Police *Fraud Prevention Guidelines* state that the following information needs to be handed over if a matter is referred to the Police:

- An accurate reconstruction of where the fraud took place
- Accounting schedules detailing the money trail
- Times, dates, places, details of money received and by whom, how recorded, how disbursed and where money was misappropriated to or from
- Accurate reconciliations of books of account showing fraudulent or missing entries
- Original documents and
- Suspect documents properly preserved.

Defamation

From time to time complainants and internal investigators express concerns about defamation. This is a complex area. Agencies and councils should get their own legal advice if they are unsure of where they stand.

In its May 2000 publication, *The Complaint Handler's Toolkit*, the Office of the NSW Ombudsman comments on defamation as follows:

"Under the Defamation Act 1974, various persons who have made complaints have the defence of absolute privilege in proceedings for defamation. This includes person who have made disclosures under the Protected Disclosures Act 1994 or complaints to the Ombudsman, ICAC or PIC."

It goes on to say:

“Any investigation report not covered by absolute privilege may nevertheless attract the defence of qualified privilege. Section 22 of the Defamation Act 1974 reads as follows:

(1) Where, in respect of a matter published to any person:

The recipient has an interest in having information on some subject,

The matter is published to the recipient in the course of giving to him information on that subject, and

The conduct of the publisher in publishing that matter is reasonable in the circumstances, there is a defence of qualified privilege for that publication.

(2) For the purposes of subsection (1), a person has an apparent interest in having information on some subject if, but only if, at the time of the publication in question, the publisher believes on reasonable grounds that the person has that interest.

What do we suggest that agencies and councils should do?

- Treat allegations of fraud confidentially from the outset
- Ensure that all investigations are characterised by objectivity and impartiality
- Always assess Information to establish if it is likely to be true
- Tell ICAC should be told if fraud is suspected
- Plan investigations properly from the start
- Remember the eight essential feature of an investigation plan
- Collect and handle evidence properly
- Conduct interviews in accordance with established procedures
- Take care when interviewing suspects to ensure fairness and the following of the rules
- Ensure that the report of the investigation forms the basis of what happens next.

What are your ideas and perspectives?

Do you think that agencies should be able to conduct preliminary investigations?

Do you think agencies should be able to conduct complete internal investigations?

Is your agency able to do preliminary or preliminary and complete investigations?

How should discovered fraud be managed?

How we see it

Fraud is an area where recidivism is high. People who commit fraud once tend to do it again. This means that any case of fraud presents an organisation with a problem that must be managed.

It is essential for agencies to vigorously respond to suspected fraud. This is to ensure that anyone considering perpetrating fraud is left in no doubt as to how the agency will react.

In a number of cases people who commit frauds have been allowed to resign without penalty. Sometimes they have even been given good references. This is done to avoid embarrassing the victim agency. But it does nothing to deter fraud. It may even tell others that the benefits of fraud outweigh the risk of such minor consequences.

There is also a public interest in not allowing wrongdoers to get away with their crimes. You must always be aware of the public interest.

The tendency to allow more senior staff to resign, and to charge more junior staff, can only serve to embolden senior staff. Senior staff, as with most white-collar workers, would generally be in a position to cause considerably more damage to an organisation than a dishonest blue-collar worker. There is a greater breach of trust.

Risk management committees should recommend appropriate actions to management.

Setting the scene

Organisations are all liable to become the victims of fraud. They must recognise this and make it clear to everyone how they will respond to fraud. A major consideration is ensuring that people considering committing a fraud believe that a lot is at risk.

The relevant staff associations and unions need to be made fully aware of what the organisation will do in response to demonstrated fraud. The role of such bodies will be in accordance with the relevant disciplinary provisions.

In making it clear from the outset how it will respond to fraud an organisation has put itself in a position to protect its resources, staff and reputation from further damage when fraud occurs.

Dealing with perpetrators

Agencies and councils should have a clearly defined policy on acting on evidence of fraud. This should be used to make it clear to staff that fraud will be treated seriously and that fraudsters will be punished.

When an investigation confirms that a fraud has taken place it may also show who is responsible. When this happens, and depending on the amount of evidence available an organisation can:

- Report the matter to the Police for action
- Initiate disciplinary action (in the case of staff).

In the case of staff, if the matter is reported to the Police it will be for them to speak to the suspect. But the organisation must act immediately to eliminate some risks. There is a number of options available including:

- Suspending the suspect with or without pay
- Transferring the suspect to other duties
- Allowing the suspect to take leave
- Allowing the suspect to resign (but not with references or gratuities)

These issues may arise once your organisation decides to interview the suspect on the basis of your suspicion.

There might not be enough evidence for criminal charges. But there might be enough evidence to support disciplinary charges and penalties.

In taking disciplinary action, you should make sure that you act according to the relevant awards, conditions and legislation. These will vary. For example, not all state agencies employ staff under the *Public Sector Management Act 1988*.

The general principles to be followed involve fairness, lack of bias and giving people the opportunity to respond to allegations.

In taking disciplinary action, it is first necessary to present the evidence to the suspect and seek an explanation. There may be two outcomes from this:

- Further information might reveal that no fraud has been perpetrated, or that the suspect is not the perpetrator. If the matter ceases to be a fraud case the remaining management questions still need to be addressed
- No adequate explanation is forthcoming. In this case the disciplinary process should continue.

From this point the procedures to be followed will be those that are set down for each agency or council. However, we suggest that:

- No references are written or given about the suspect
- Any requests for references are referred to an appropriate manager
- The suspect is not permitted to enter the organisation's premises uninvited (other than to conduct business with the organisation).

Preventing further fraud

It is important that any fraud is not repeated. You also need to ensure that similar circumstances do not arise again. There may be potential for them to arise in other parts of the organisation. These should be identified and anticipated.

When an investigation reveals that a fraud has taken place it should also uncover how it was done. This should show up the weaknesses in the relevant systems. These should then be fully assessed and remedial action taken.

The lessons learned from the uncovered fraud should be applied throughout the organisation. The details should be provided to all relevant line managers so that they can examine their operations for similar circumstances and risks.

Supervisors and colleagues of the perpetrator should be encouraged to try to see if they could have noticed something sooner. Anything they think of might assist in detecting or preventing other frauds.

If there would be enough interest, the story should be told to other agencies so they can look at their arrangements and risks. For example, a fraud committed at a council swimming pool would be of interest to most councils in NSW.

What do we suggest that agencies and councils should do?

- Agencies need to manage the situation when fraud is uncovered
- A risk management committee should have overall responsibility for an investigation
- Even if a fraud is confirmed but no perpetrator is identified the situation must not be allowed to go un-addressed
- Lessons learned from frauds must be applied throughout an organisation
- Agencies need to respond vigorously to suspected fraud.
- It is not in the public interest, or the interest of organisations', for perpetrators of fraud to escape consequences
- Organisations must establish their position and reaction policies before fraud is discovered
- All parties must fully understand what will happen in the case of fraud
- Organisations must ensure that frauds do not recur
- If enough evidence is uncovered, Police should be contacted when fraud occurs
- Disciplinary action should be taken where practicable
- Relevant awards, rules and legislation must be complied with at all times
- Fairness must be shown at all times
- It is not necessary for proof beyond all reasonable doubt to be found before action can be taken
- Organisations have an obligation to do what they can to prevent a perpetrator offending again from a position of trust.

What are your ideas and perspectives?

Do you think the features listed here are important in fraud prevention?

Are there any legitimate advantages in keeping frauds quiet?

Can you see any difficulties with dealing firmly with fraud?

Have you any suggestions for other things to include in this section?

What about these suggestions?

Suggestion: Policing

The NSW Police say that they expect organisations that can afford to investigate fraud themselves to do so. This is likely to mean that all public agencies and councils will have to do, or commission, their own investigations.

Questions

What is the proper role for the NSW Police to play on fraud?

Will your organisation be able to investigate suspected fraud in the future?

Suggestion: Compliance

The Commonwealth Government is to impose fraud control requirements on Chief Executive Officers of agencies. These are intended to improve fraud control by increasing the public scrutiny of agencies' activities.

Under these arrangements agencies will be required to:

- Address fraud control in their annual reports
- Develop an overall fraud control strategy.
- Report fraud control initiatives to Ministers.

In NSW, the proposed rewrite of the *Public Finance and Audit Act* may be an opportunity to impose on agencies a responsibility to:

- Adopt fraud prevention plans
- Report all frauds to ordinary meeting of their governing bodies
- Report all frauds and fraud prevention activities in their annual reports.

Questions

Is it a good idea to require such steps?

Would it be difficult to comply with such requirements?

Suggestion: Investigation standards

The Commonwealth Government has also produced standards for fraud investigations. The standards claim to describe a best practice approach to investigations. They include a set of modules that together comprise the standards that agencies must be able to meet.

The standards are linked to investigator competencies established by the Commonwealth Fraud Training Advisory Committee. The standards describe what an investigator must be able to do.

The intention is that all agencies use investigators with those competencies when investigating fraud. The NSW Audit Office holds a similar view.

Questions

Does anyone your organisation have any formally qualified investigators?

Do you think a formal requirement that people hold a qualification is appropriate?

Would your agency be interested in participating in a short course intended to develop those skills?

How do you think such training should be funded?

Suggestion: Incidence

Fraud reporting might be a problem. Fraud is generally thought to be on the increase. It is large part of the ICAC's caseload. But the number of fraud cases reported to the Police by agencies and councils is quite low. It is likely that a significant amount of fraud is being detected but is not being reported to the Police. It is also possible that a significant amount of fraud is going undetected.

Questions

How many cases of suspected fraud have occurred in your agency in the last three years?

How many such suspicions proved true?

Were you able to respond satisfactorily?

Was your organisation able to eliminate the risk adequately?

What happened in the end?

Suggestion: Fraud database

It has been suggested that there should be a central fraud database. It would contain details of all proven and suspected cases of fraud in NSW. The detail would include the identity of the suspected fraudsters. It would probably be held by the Police and could operate as a reference for organisations thinking of employing people in high-risk positions.

Questions

Would such a database be helpful?

What are some of the risks in operating such a database?

Who should have access to such a database?

Should the database only contain information on convicted fraudsters or should it include other things (e.g. admissions in exchange for being allowed to resign)?

Suggestion: Discussion paper

There is a growing realisation that fraud is a problem for all organisations in the State. The ICAC has a responsibility to assist agencies and councils to manage the risk of fraud and to manage the situation when fraud occurs. This discussion paper is intended to get the informed view of as many people in NSW agencies and councils as possible. The ICAC will then publish Fraud Response Guidelines based on the outcome of this process.

Questions

Do you think that fraud poses as big a threat as this paper implies?

Do you think that this discussion comes at the right time?

Do you think that this discussion is worthwhile?

Do you think that a guideline publication, modelled on the approach and order of presentation in this paper, would be helpful?

Do you think the ICAC should produce two specific publications, one for State agencies and one for local councils?

Do you have any suggestions for what might be a better approach to publishing guidelines?

Is there anything that we have not raised that you would like discussed?

What to do with the answers?

There are four ways that you can send your answers, comments and suggestions to the ICAC:

Email: icac@icac.nsw.gov.au (mentioning fraud in the subject box)

Mail: ICAC Fraud Discussion
GPO Box 500
Sydney NSW 2001

Fax: (02) 9264 5364

Phone: (02) 8281 5999 (ask to speak to the duty CP Officer)

Please ensure that your contribution is received at the ICAC by COB Monday 10 June 2002.

Where did we get our information?

In preparing this paper we got information from a number of places. Much of it is from our own sources, records, and experience. We also spoke to people in other organisations and sought their views.

We also got information from publications and papers. Those are listed below. Some of them also contain or refer to some fraud prevention tools.

Many are available on web pages such as those of the government agencies responsible. Those and other sites contain further information on fraud risk management and corruption prevention generally.

The ICAC thanks those responsible for the following publications:

Atkins, Liz (2002). *Managing ID Fraud*, Preventing Fraud and Corruption in Government, Conference.

Attorney-General's Department (2001). *Commonwealth Fraud Control Policy and Guidelines, Consultation Draft NO. 2*.

Audit Office of NSW (1988). *Performance Audit Report, Fraud Control, Status Report on the Implementation of Fraud Control Strategies*.

Audit Office of NSW (updated 1999). *Self-Audit Guide for Assessing Best Practice in fraud Control Strategies*.

Audit Office of NSW & NSW Premier's Department (1993). *Fraud Control: Developing an Effective Strategy, Volume 3 Diagnostics*.

Australian National Audit Office (2000). *Survey of Fraud Control Arrangements in APS Agencies*.

Commonwealth Law Enforcement Board (1996). *Commonwealth Fraud Investigation Standards Package*.

Commonwealth Law Enforcement Board (updated 1996). *Best Practice for Fraud Control Fraud: Control Policy of the Commonwealth*.

Criminal Justice Commission (1993). *Corruption Prevention Manual*.

Elliott, Derek of District Audit (2001). *Assessing, Influencing, Changing Anti-Fraud Cultures*, 10th IACC Conference, Prague.

Independent Commission Against Corruption (1997). *Internal Investigations*.

NSW Police Service On-Line (2001). *Fraud Prevention Guidelines*.

Independent Commission Against Corruption (1998). *Ethics the key to good management*.

-
- Independent Commission Against Corruption (2001). *The First Four Steps*.
- Independent Commission Against Corruption (2001). *Annual Report 2000-2001*.
- Independent Commission Against Corruption (2001). *Minimising Corruption: some lessons from the literature*.
- KPMG Forensic Accounting (1999). *1999 Fraud Survey*.
- NSW Police Service (2000). *Future Directions 2001-2005*.
- NSW Police Web Site (2002). *Fraud Prevention Guidelines*.
- NSW Treasury (1997). *Risk Management and Internal Control Toolkit*.
- O'Donnell, Christopher (June 1998). *The Elements of Criminal Fraud – Recent Developments*. Crime Law Journal, Volume 22, pp140-150.
- Office of the NSW Ombudsman (2000). *The Complaint Handler's tool Kit*.
- Office of the NSW Ombudsman (2000). *Investigating Complaints: A manual for investigators*.
- Office of the NSW Ombudsman (2002). *Protected Disclosure Guidelines (4th Edition)*.
- Schnedier, Anton (2002). *Assessing the impact of new control reviews in the Commonwealth Fraud Control guidelines*, Preventing Fraud and Corruption in Government, Conference.
- Smith, Russell G (1998). *Best Practice in Fraud Prevention* in Trends & Issues in Crime and Criminal Justice, No100, Australian Institute of Criminology.

