Fraud Control
Current Progress and Future Directions

guidance on better practice

February 2005
Introduction

Given the size of the NSW public sector, the potential for fraud could run into billions of dollars if not properly managed. It is an area of risk that warrants close and ongoing attention. Over the last decade, we have responded by issuing three performance audits and a comprehensive guide to better practice on this topic.

In conducting financial audits, there is now an Auditing Standard that requires us to seek annual assurances from every agency concerning the adequacy of their arrangements for fraud control. This latest performance audit provides a further report card on the extent to which the NSW public sector is managing its fraud risks.

This Report provides updated guidance on improving arrangements for fraud control both at a whole-of-government level and at the agency level.

This guidance on better practice is reproduced from our performance audit report *Fraud Control: Current Progress and Future Directions*. The full report is available on our internet site: [http://www.audit.nsw.gov.au/](http://www.audit.nsw.gov.au/)
A Simplified Strategic Management Framework for
Fraud Control for Use by Audit Committees

In our 1994 Guide, one of the 10 key attributes for an effective fraud control strategy was “responsibility structures” (Attribute 2). We gave this a very high level of importance because there were indications that, at that time, responsibility for fraud control was not clear in many agencies.

This is not an unusual problem. There are many issues in organisations for which this can be said. Risk management in general, for example. With issues such as this, that are principally line management responsibilities, the challenge is a classic governance one: how to provide assurance that vital aspects of how the organisation operates are working as required?

In our 1994 Guide we said “a comprehensive responsibility structure must be developed to implement and give effect to the agency’s fraud control strategy.” We recognised the responsibilities of line management, and provided guidance on how agencies could approach clarifying and reinforcing this.

In the case of issues such as fraud control and risk management (amongst others), experience has led to a widely-held view that there is also a need to allocate some specific responsibilities for oversight. This can be organised in a number of ways, but in 1994 we suggested a fraud control committee as a potentially useful means. At that time, audit committees were not widespread in NSW agencies. Today,
audit committees are regarded as a key component of governance for all forms of organisations.

In obtaining feedback from expert practitioners about their practical experience with implementing fraud control, this evolution in the extent and role of audit committees was raised. Most agencies have chosen to include a responsibility for their audit committee to periodically review the effectiveness of the agency’s fraud control strategy. We support this approach.

However, practical experience appears to suggest that in undertaking their review role, audit committees find the current guidance material too detailed. This makes sense, since the material was written for fraud control practitioners. Even the checklist material (Volume 3 of the 1994 Guide), and Self-Assessment Audit Guide (1998), was pitched to support the detailed development, and detailed internal/external audit, of fraud control strategies. It is clear that we need to find a better way to assist audit committees to perform their crucial review role.

The competency standards for fraud control developed in the Commonwealth public sector refer to elements of prevention, detection and investigation. Such a classification framework appears to have taken favour with management, as it simplifies the many elements in a common-sense way.

It provides a useful classification system for applying the notion of an holistic integrity-system approach (a concept developed by Transparency International) to the specific area of fraud control.

This simple framework provides a high-level frame of reference to discuss and evaluate fraud control efforts that we think is ideally suited for use by audit committees.

A simple way for Audit Committees to question and examine their agency’s fraud control performance and to support the agency representations required by AUS210

![Diagram of fraud control framework]

- **Prevention**
- **Detection**
- **Investigation**
As a test of using this framework, we applied it during this audit. It provides a simple way of organising and focusing thinking, questioning and research material. What follows is the product of our use of this method to identify, on a whole-of-government basis, areas of comparative weakness and areas of lag in adopting best-practice initiatives.

The intuitive appeal of this tool, its simplicity of use, and its effectiveness in producing an action-agenda, convinced us that it would be of great assistance to an audit committee using it for a single-agency analysis.

Fraud control practitioners will continue to use more detailed frameworks, as described in the next chapter. But this provides a tool suited for an audit committee in addressing the agency’s fraud control representations required by the Auditor-General under AUS 210.

**Prevention**

Prevention consists of an organisation:

- determining the fraud risks to which it is exposed
- putting in place policies, systems and procedures to deal with these risks.

The results of research suggest that prevention is an area where many agencies have applied considerable effort and are doing quite well. This is very important, as prevention is a critical dimension of fraud control. We strongly encourage agencies to maintain this level of attention.

But what, if anything, more should agencies be doing for effective fraud prevention?

**Hot tips for improving prevention**

Examining AS 8001, our own ten-point model for fraud control, and current thinking on best practice, we have identified a key action in the area of prevention that we would recommend all agencies closely consider: pre-employment screening.

**Pre-employment screening**

Pre-employment screening is increasingly being used by organisations in both the public and private sectors.

We note that some public sector organisations now routinely ask prospective employees to agree to pre-employment checks, which may involve criminal records checks as well as speaking to current or former supervisors.

There have recently been high profile cases in both the public and private sectors that have drawn this issue to the attention to HR managers.
Some of these cases relate to fraudulent academic credentials, positions held and so forth. Others will conceal criminal records and other matters of significant concern to a prospective employer.

Perhaps most importantly of all, pre-employment checks effectively stop perpetrators of fraud moving from organisation to organisation and continuing their less than desirable behaviours in more than one location.

**Recommendation**

To further improve performance in the area of fraud prevention, we recommend that agencies consider adopting, or enhancing, pre-employment screening practices.

**Detection**
Detection consists of an organisation:

- implementing policies and systems to find out what is happening in practice. This involves receiving information (passive detection) and proactively searching for indications (active detection)
- reviewing high and medium risk activities (from a fraud control perspective) to which it is exposed to identify untoward behaviours
- sampling low risk activities to determine if they remain low risk and/or whether untoward behaviours are taking place.

The results of research suggests that of all aspects of fraud control, the area most in need of improvement is detection. In general, NSW agencies are not as strong in this area as current thinking suggests they should be.

**Hot tips for improving detection**

Computerised accounting systems are now thoroughly embedded into the day-to-day operations of all public sector organisations in NSW. From an accounting perspective, this means that all financial transactions being undertaken by the organisation are recorded and stored for future reference. Working “around the system” is no longer an option. This provides a useful opportunity for fraud detection.

**Data mining**

In simple terms, all that needs to be done is to ask meaningful questions of the accounting and financial systems to see what is happening. The emergence of sophisticated data mining tools has made such analysis possible at a relatively modest cost. Helpfully, some of the most effective data mining tests are very simple ones to run.
Some things will be easier to find than others. For example, checking whether invoices have been split into smaller amounts so that none exceeds public sector guidelines on expenditure has proven to be a worthwhile test. As has checking for duplicate payments and multiple vendor names (with slight variations). Other tasks will require more sophisticated approaches, which are also available through the rapidly developing area of forensic accounting and investigation.

Over time, data mining tools will become more well-known and widely available and we encourage agencies to consider where they might fit into more robust strategies to deal effectively with detecting corruption. They have a proven value-add, and are relatively inexpensive.

Data mining by line management

However, fraud detection computer analytical tools should not be seen as the domain of fraud control specialists, investigators and auditors. Such groups will certainly make highly effective use of such tools (and it should be regarded as standard practice). However, beyond that, a strong sign that an organisation has effective fraud detection in operation is the routine use of such tools as a part of everyday line management.

We strongly encourage agencies to build the capacity into their systems for detection routines that provide line management with routine reports and provide line management with simple tools.

Fraud reporting systems

Another proven detection method is the observations of staff, contractors, suppliers and customers. Experience suggests that if something untoward happens in an organisation, there is likely to be someone who knows something about it. But how likely are they to tell anyone? And how easy is it for them to do so? Unfortunately, experience also suggests that few organisations do this well, and thus fail to make effective use of one of the most potent detection tools available.

Like data mining, the development of effective corruption reporting systems has become a specialist industry with considerable research and development being undertaken. Advances have been made in systems to receive and process information about alleged improper actions, in ways that provides security and confidence to those providing such information as well as processing it efficiently.

Our survey shows that most agencies have complied with their obligations for reporting, and have instituted reporting systems, particularly for protected disclosures. However, in examining this issue more closely against best practice standards it is not apparent that this valuable channel has been developed sufficiently in most agencies to reach its potential.
There is evidence to suggest that making improvements to these systems will generate substantial value to agencies, and we encourage agencies to carefully consider this aspect of their detection regime.

**Recommendation** To further improve performance in the area of fraud detection, we recommend that agencies:

- adopt, or enhance, their use of data mining as a routine element of line management review of operations
- require their audit and investigation teams to apply relevant data mining and forensic investigation tools
- enhance their processes for receiving reports from staff, contractors, suppliers, customers and stakeholders.

**Investigation** Investigation consists of an organisation systematically and thoroughly reviewing to required standards, and in compliance with required rules, actions and events which are deemed to be “of concern”, then subsequently:

- imposing appropriate sanctions and/or reporting the matter to other investigating agencies for action (ICAC, Police etc)
- recommending strategies and actions to overcome perceived deficiencies in policies and processes.

Investigations is a strong area of the fraud control framework in the Commonwealth which NSW does not enjoy.

When issued some years ago, the Commonwealth’s Investigation Standards (and accompanying model procedures) provided best practice for investigations. The Standards apply to all forms of investigation, and outline the written procedures that each agency should have in place to perform an efficient and effective investigation. The model procedures are minimum arrangements and Commonwealth agencies must have in place procedures that are consistent with or exceed the model procedures.

In introducing the Standards, the Australian Federal Police conducted a rolling program of quality assurance reviews to examine whether agencies were conducting their investigations to an adequate standard.

Commonwealth officers working in the fraud control area must also be trained and certified to formal competency standards.

In the absence of a comparable regime in NSW, investigations are not undertaken to a uniform standard. Some agencies have outsourced investigations, however, this is not a guarantee of uniformity, or even necessarily of quality.
Hot tips for improving investigations

As part of their fraud control strategy, we encourage NSW agencies to adopt recognised standards for investigations. We also encourage agencies to consider the extent to which investigations, whether conducted in-house or outsourced, are quality assured against those standards.

Recommendation

To further improve performance in the area of fraud investigation, we recommend that in undertaking investigations (either by staff or outsourced providers) agencies:

- adopt recognised investigation standards
- include appropriate quality assurance arrangements for fraud investigations.
Directions for Change:
Assistance for Fraud Control Practitioners

Current challenges for fraud control

The Audit Office’s ten-point model for fraud control has now been available for 10 years. It is widely recognised in both the public and private sectors as an effective approach to the subject, and has formed the basis of frameworks developed for some other jurisdictions. However, the nature of fraud continues to evolve, as does its prevention, detection and investigation.

In addition to the survey, our method included a range of other research actions. One of these was to convene a focus group of experienced fraud control practitioners to undertake a number of tasks, including identifying significant issues impeding the implementation of effective fraud control strategies.

We had already identified 25 issues of concern from our own research and the survey. Our expert group extended this list to 45. Such widely varying issues indicate just how complex it is to effectively implement fraud control strategies in individual organisations.

Priority issues

The focus group ranked the “top ten” issues as:

1. Fraud risk assessment practices being poor in agencies
2. Ethical behaviours by staff
3. Responsibility in times of organisational change
4. Training for managers about how to manage the issues of fraud and corruption (equal with)
5. Lack of systematic risk assessment within agencies
5. Wide spread introduction of new technology, with greater delegation of decision making (equal with)
5. Management of confidential / commercially sensitive information (equal with)
5. Changing control structures
6. IT systems have appropriate audit trails, but auditing does not take place often enough/at the required standard (equal with)
6. Technology systems insufficiently robust
7. Early warning signs of fraud often either ignored or not acted upon quickly enough (equal with)
7. Internal control systems increasingly being “short cut” to get things done in a hurry (equal with)
7. Lack of commitment by agency senior executive to issue of fraud control
8. Training for staff in ethical behaviours (equal with)
9. Smaller agencies need different approaches, support than the medium to larger sized agencies (equal with)
10. Managing the aftermath of investigations.

A series of common themes emerged from the focus group, described in the diagram below:

Current and Emerging Issues in Implementing Effective Fraud Control

The fraud control practitioners at the focus group indicated a strong desire for us to retain the fraud control model that had been in operation since 1994, but also to update and refine it based on experience and current thinking about priority issues for fraud control. We have done so.

To provide fraud control practitioners with an updated source of guidance we have:
- fine-tuned our 1994 ten-point model’s Attributes of Best Practice
- better explained the aim of each Attribute so that they are as easy as possible to implement
- provided examples of what would be seen in organisations who have successfully implemented the attribute (indicators of success)
- provided “hot tips” to help organisations take immediate actions to improve the management of fraud control.
Those familiar with the model that agencies have been using for the past ten years, will notice some change:

- there have been changes to the names of some of the current attributes to reflect a move to an “integrity systems” approach (a concept coined by Transparency International)
- two existing Attributes have been combined (Attributes 6 and 7) to form a single Attribute: “Notification Systems”
- Attribute 7 (Detection Systems) is new.

The 2004 revision of our ten attributes of best practice in fraud control follows.

**Recommendation**  
To further improve overall performance with managing fraud control, we recommend that Audit Committees direct the agency’s internal audit and/or investigations functions to review and update the agency’s fraud control strategy against the 2004 revision of the Audit Office’s ten attributes of best practice for fraud control. In so doing, areas identified by this audit as warranting particular attention include:

- pre-employment screening practices
- strategies to make staff, customers and the community aware of the agency’s commitment to fraud control
- the use of data mining as a routine element of line management review of operations
- the use of relevant data mining and forensic investigation tools by audit and investigation teams
- processes for receiving reports from staff, contractors, suppliers, customers and stakeholders
- the regularity and robustness of fraud risk assessments
- recognised standards for investigation activities
- appropriate quality assurance arrangements for fraud investigations.
2004 Revision of the Ten Attributes of Best Practice in Fraud Control

Attribute 1  Integrated Macro Policy

**Aim of Attribute** is to ensure that:
- agencies have in place the necessary policies, systems and procedures to minimise fraud in all places, and at all levels, of an organisation
- policies, systems and procedures respond, and are proportionate, to the fraud risks faced by the organisation.

**Indicators of Successful Implementation:**
- Policies, systems and procedures are based on assessed fraud risks
- Policies, systems and procedures have been updated in the last 2 years.

**Hot Tips**
- Confidential/commercially sensitive information needs to be actively monitored
  - Does it comply with legislative standards?
  - Does it comply with commercial standards?
  - How secure is the commercial information?
- One policy approach won’t fit all
  - Smaller and medium size agencies will take different approaches to larger agencies
- One definition of fraud won’t fit all agencies
  - Each agency needs to define what fraud means in the context of its core business activities
- There is a myth that large amounts of money need to be spent to deal effectively with fraud control:
  - In reality, agencies can take some simple steps and be confident that they are able to exercise effective management over their risks in a controlled way.
Attribute 2  Responsibility Structures

**Aim of Attribute** is to ensure that:

- There is clear accountability and responsibility for implementation and monitoring of the fraud management strategy
- This accountability is well known by all staff at all levels and in all places of the organisation
- There is a common understanding that everyone in the organisation has a role to play in effective fraud management.

**Indicators of Successful Implementation:**

- Position descriptions have appropriate fraud control elements incorporated
- Managers and staff are able to articulate their fraud control responsibilities
- Audit Committee periodically reviews the effectiveness of the agency's fraud control strategies.

**Hot Tips**

- Ensuring responsibilities and accountabilities remain clear in times of organisational change
  
  As part of finishing any restructure, agencies need to ensure that responsibilities for fraud are considered in creating/revising position descriptions
- Widespread introduction of new technology means that there is greater delegation of decision making
  
  When introducing new technology, there is a need to ensure that there are still appropriate checks and balances in decision making
- “Tone at the top” sends out important messages to managers and staff
  
  Executive management need to lead fraud control in their agency by their own behaviours, driving the issue of fraud control through the organisation
- Training for managers in managing fraud
  
  Managers need the knowledge and skills so they can effectively discharge their executive responsibilities for managing fraud
- Clarity in management responsibilities/actions for supporting staff
  
  Managers need to be clear about their roles and responsibilities for supporting staff in dealing with the many and varied fraud related issues that emerge in the workplace
- Flattened organisational structures mean that there are fewer middle level managers to enforce internal controls
  
  With fewer levels of management, and an outcomes focus, it is easy to override internal controls to “get things done”. Actions such as this have been shown to be significant contributors to instances of major fraud in organisations.
Attribute 3  
Fraud Risk Assessment

**Aim of Attribute** is to ensure that:
- A separate fraud risk assessment is undertaken by the organisation
- The fraud risk assessment quantifies the level, nature and form of the risks to be managed
- Actions will be taken by the organisation to mitigate the risks identified in the fraud risk assessment.

**Indicators of Successful Implementation:**
- Risk assessment undertaken in last 2 years
- Risk assessment covers internal and external operating environments
- Risk mitigation actions assigned to individual members of management and/or staff for action.

**Hot Tips**
- General risk analysis is insufficient:
  - Fraud risk assessment needs to be undertaken separately from general risk management exercises
- Get staff thinking about fraud risks in all business units
  - Quality of risk assessment processes needs to be the best possible. Staff at all levels and in all places need to be involved
- Fraud risk assessment needs to be undertaken on a regular basis
  - If your fraud risks analysis is over two years old, then it needs a fresh assessment.

Attribute 4  
Employee Awareness

**Aim of Attribute** is to ensure that:
- All employees understand the ethical behaviours required of them in the workplace
- Training programs in ethical behaviours are in place across the organisation
- Training deals with the fraud risks faced by individuals in their workplaces.

**Indicators of Successful Implementation:**
- Ethical behaviour is included in organisation induction programs for new staff, temporary staff, contractors etc
- Employees are able to articulate the fraud risks they are required to deal with in the workplace
- Employees are able to articulate the actions that they need to take to respond to fraud in their workplace.
**Hot Tips**

- The term “employees” covers a lot of different people:
  - Have you thought about part-time, temporary and casual staff? Contractors? Consultants?
- Ethical behaviours are a key to getting fraud control “right” in an organisation:
  - Staff need to know exactly what is expected of them in the workplace
- Training for staff in ethical behaviours:
  - Just as managers need training in ethical behaviours, so staff need training too
- Difficulty of getting the message acted on “in the field”:
  - Training is not sufficient: there needs to be encouragement for appropriate workplace behaviours.

**Attribute 5  Customer and Community Awareness**

**Aim of Attribute** is to ensure that:

- Customers and the community understand that the organisation will not accept fraudulent dealings/transactions
- Customers are aware of the consequences of fraudulent dealings/transactions
- Information is available to customers about the quantity, quality and timeliness service delivery.

**Indicators of Successful Implementation:**

- Customer service standards in place
- Transactions with customers audited for fraudulent behaviour, consistent with the assessed level of fraud risk of the transaction
- Regular reporting to community of actions to prevent and control in the organisation.

**Hot Tips**

- Publicising poor behaviours and their consequences:
  - Customers and the community need to know what will happen should attempts be made to interact fraudulently with the organisation
**Attribute 6** Notification Systems

**Aim of Attribute** is to ensure that:
- Policies, systems and procedures are in place to encourage the reporting of suspect behaviours
- Fraud notification systems give the complainant the opportunity to report the suspect behaviours anonymously
- “Whistle-blowers” are protected by the organisation
- Policies, systems and procedures give equal opportunities to managers, staff, contractors, consultants, customers, suppliers etc to notify the organisation of suspect behaviours.

**Indicators of Successful Implementation:**
- There is regular testing of the fraud notification system to ensure that notifications are recorded and passed onto the appropriate manager for action
- Fraud notification system generates quarterly reports into both number and nature of internal and external complaints received
- Actions taken to resolve notifications of suspect behaviours reported quarterly to the executive of the organisation
- “Whistle-blowers” report satisfaction with the actions taken by the organisation to resolve their concerns about suspect behaviours.

**Hot Tips**
- Notification systems are tricky things to get right internally: Outsourcing notification systems to third party providers may be worth considering.

**Attribute 7** Detection Systems

**Aim of Attribute** is to ensure that:
- Available data is thoroughly monitored and reviewed to ensure that irregularities and warning signals are picked up at a very early stage and flagged for further detailed review
- Internal audits regularly examine samples of medium and high risk financial decision making across the organisation
- Audit Committees make decisions, based on risk, about key systems and decisions to be audited
- Outcomes of audits are reported to executive management on a quarterly basis.
Indicators of Successful Implementation:

- The organisation is routinely using data mining tools in detecting fraudulent behaviours as part of line management review
- Audit and investigation functions employ advanced data mining and forensic review tools
- Medium and high risk transactions are audited on a regular basis for probity
- Audit report recommendations are followed up
- There is clear accountability for implementation of audit report recommendations.

Hot Tips

- Individual organisations have all the records they need to detect fraud:
  - IT systems have appropriate audit trails, but auditing does not take place often enough/at the required standard
- Agencies are increasingly relying on technology to provide the efficiency and effectiveness required of the agency:
  - Is the use of technology sufficiently robust from a fraud control perspective?
- Major fraud can be avoided:
  - Rather than ignoring early warning signs of fraud or not acting on them quickly enough, if in doubt you should act NOW
  - Probity audits should regularly examine a sample of medium and high risk decision processes across the organisation
- The need to achieve outcomes needs to be balanced with due process:
  - When you short-cut internal controls, you are exposing yourself to significantly larger risks of fraud happening
- Technology can now produce “flawless” fraudulent documents:
  - What has your organisation done to think through this issue? Does it rely on “standard” third party documents? How reliable are these now?
- Introduction of large scale technology dependent finance systems is a major risk for organisations:
  - Is the finance system able to produce meaningful management information at the time required?
- Existing levels of fraud unable to be easily quantified:
  - There is a view that “if it can’t be quantified, there isn’t a problem”. Is this a realistic point of view?
Attribute 8  External Notification Systems

Aim of Attribute is to ensure that:
- Agencies have policies which clearly identify the nature of suspect actions which require reporting to the Police, the ICAC, the Ombudsman etc
- External notification takes place as required in light of the above legal and policy requirements.

Indicators of Successful Implementation:
- Agency provides information in annual report about number of suspect incidents referred to Police, ICAC, Ombudsman etc for action
- Results of those actions reported to the community.

Hot Tips
- Organisations can become embarrassed about becoming the victim of fraudsters:
  - Treating fraudsters with leniency, allows them to move from organisation to organisation. This is to be avoided at all costs.

Attribute 9  Investigation Systems

Aim of Attribute is to ensure that:
- Procedures and other appropriate support (including training, where required) is provided to staff undertaking investigation activity on behalf of the organisation
- Investigation actions undertaken should be consistent with commonly used investigation standards
- Where appropriate expertise is not available internally, then external assistance should be sought
- All investigations consider what improvements can be made to policies, systems and procedures within the organisation
- All investigation reports are referred to the audit committee or an equivalent, and the organisation’s senior executive, for action.

Indicators of Successful Implementation:
- The agency has adopted recognised Standards for conducting investigations
- Investigations are audited for due process on a regular basis
- Investigations use appropriate data gathering and analysis mechanisms to come to valid conclusions
- Investigation results are referred to the audit committee and the organisation’s senior executive for action.
**Hot Tips**

- Investigations are tricky to undertake and manage:
  - Don’t assume that your audit staff are fully competent in this specialised area
  - Perhaps you may wish to consider training relevant staff against competency standards that are available in this area?
  - Investigations need to ensure that there is even-handedness for both complainant and those accused.
- Is your organisation using an appropriate approach to investigations?
  - There are investigation standards (eg. ICAC, Commonwealth) that can be used to ensure that processes are at “best practice” standards
- Increasing reliance on external expertise:
  - Outsourcing does not guarantee quality. This is still your responsibility
  - What about training internal staff to undertake this most sensitive of tasks? This both builds up organisational expertise and also lessens reliance on external providers.

**Attribute 10  Conduct and Disciplinary Systems**

**Aim of Attribute** is to ensure that:
- Employees understand that fraud will not be tolerated and that perpetrators will face disciplinary action
- Employees have access to written information to assist them understand their ethical obligations
- Approaches will be developed that are consistent with both perceived risks and the organisation’s approach to human resources management.

**Indicators of Successful Implementation:**
- Employees are able to articulate their obligations in regard to ethical behaviours
- Managers able to articulate the steps that need to be taken in disciplinary circumstances.

**Hot Tips**

- Codes of Conduct are critical:
  - Lack of one or one that is poorly implemented will lead to poor outcomes for the organisation
- Consistency in sanctions:
  - Unless everyone is treated the same way, the organisation is left vulnerable to charges of victimisation/favouritism.