

# **Strategic Control Plan in Dealing with Fraud & Corruption**

*Academic paper by Peter John Lynch  
(PJL) of Lynch Investigations &  
Countermeasures Pty Ltd.*

*Grad. Cert. Fraud Investigations (CSU)  
Adv. Dip. Gov Fraud Control Management  
Adv. Dip. Security Risk Management  
[www.pjlinvestigations.com.au](http://www.pjlinvestigations.com.au)*



## Contents

<b>Introduction.....</b>	<b>page...1</b>
<b>Establishing Fraud Risk Management.....</b>	<b>1</b>
<b>Fraud Risk Management Policy.....</b>	<b>2</b>
<b>Risk Management Process.....</b>	<b>5</b>
<b>Identification of Key Personnel.....</b>	<b>6</b>
<b>Establish The Fraud Risk Management Context.....</b>	<b>6</b>
<b>Identify Key Players.....</b>	<b>6</b>
<b>Setting The Criteria.....</b>	<b>7</b>
<b>Identify Risks.....</b>	<b>7</b>
<b>Analyse Risks.....</b>	<b>7</b>
<b>Assess and Prioritise the Fraud Risks.....</b>	<b>7</b>
<b>Manage The Risks.....</b>	<b>8</b>
<b>Evaluate the Fraud Risk Management Options.....</b>	<b>8</b>
<b>Fraud Risk Management Plans.....</b>	<b>8</b>
<b>Linkage to Other Governance Processes.....</b>	<b>9</b>
<b>Procedures for Reporting Fraud and Corruption.....</b>	<b>9</b>
<b>Procedures for Handling Allegations.....</b>	<b>10</b>
<b>Procedures for Investigating Cases.....</b>	<b>10</b>
<b>Procedures for collecting information.....</b>	<b>11</b>
<b>Awareness Raising and Training.....</b>	<b>12</b>
<b>Procedures for evaluating success of Strategy.....</b>	<b>12</b>

## Introduction

The purpose of this Fraud Risk Management Plan is to advise managers and staff of the process for responding to and dealing with possible fraud and over servicing, which may arise during the processes in providing customer service in selling of products and services.

The Fraud Risk Management Plan outlines a methodology by which the risk of fraud can be identified analysed and assessed provided along with monitoring and review processes. Fraud risk management is part of the company's culture; the fraud risk management policies have active support of the organisation's Senior Management.

Good fraud risk management has regular reviews of procedures, delegations and a member of Senior Management to facilitate the effective management of fraud risk and to ensure a commitment to the organisation's policy and procedures.

Valued fraud risk management promotes fraud awareness within the organisation. The effectiveness of this fraud control plan will depend upon the appropriate mix of prevention and detection measures.

## Establishing Fraud Risk Management

Definitions are provided to assist personnel involved with the fraud control program. Fraud is the use of deceit to obtain an advantage or avoid an obligation.

Risk management encompasses the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

Risk is the chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood.

## Fraud Risk Management Policy

**Introduction:** The organisation is committed to sustaining an honest and ethical environment. The organisation is responsible and accountable for providing measures by which to manage or eliminate dishonesty, fraud and corruption in the workplace. There is to be a commitment by all of the organisation's staff to fraud risk management.

**Rationale:** In line with the Crimes Act 1900, WOHS and the organisation's security policy, this document is confined to a process of identifying, assessing and managing fraud risks likely to effect the attainment of profitability, safety, reputation, shrinkage levels and maintenance of these goals.

**Aim:** The identification of fraud risks and their subsequent management.

**Objectives:** The control of fraud within the organisation's framework.

**Strategy:** The fraud risk management process shall consist of identifying the risks, ranking the likelihood and consequence of occurrence along with the management of the risks, including action plans aimed at reducing the identified risk and communicating risk to all staff.

**Responsibility:** The senior management shall appoint a responsible person to manage the fraud risk management process. The responsible person shall oversee and implement the fraud risk management process with reporting monthly of the organisation's progress. The responsible person will review the fraud risk management program to ensure the effectiveness of control measures and risk priorities are monitored to ensure appropriateness.

It shall be the responsibility of everyone in the organisation to report suspected dishonesty, theft, fraud, corruption, waste and any other form of deceit of the organisation.

Failure of disclosure of information regarding suspicion of theft, fraud, corruption, waste or any other form of deceit of the organisation will be dealt with by disciplinary procedure.

**Implementation:** The responsible person shall consult with personnel responsible for the administration or implementation of the security arrangements to assist in the identification of fraud risks.

Accepted risks identified shall be monitored, unaccepted risks shall be ranked with an appropriate action plan developed for controlling and monitoring. A register of identified risks shall be maintained, with a review of the fraud risk management arrangements that will take place at least every two years or

whenever warranted by disclosure of a risk not identified previously or upon the identification of a deficient risk treatment plan.

**Training:** To achieve the implementation of the fraud risk management plan, the responsible person shall have obtained relevant levels of training, suggested Tertiary Diploma in Fraud Control and Investigation. All staff shall receive an awareness program, specific program or specific training in fraud risk management as it affects the profitability, security, safety, shrinkage levels and maintenance of these goals of the organisation.

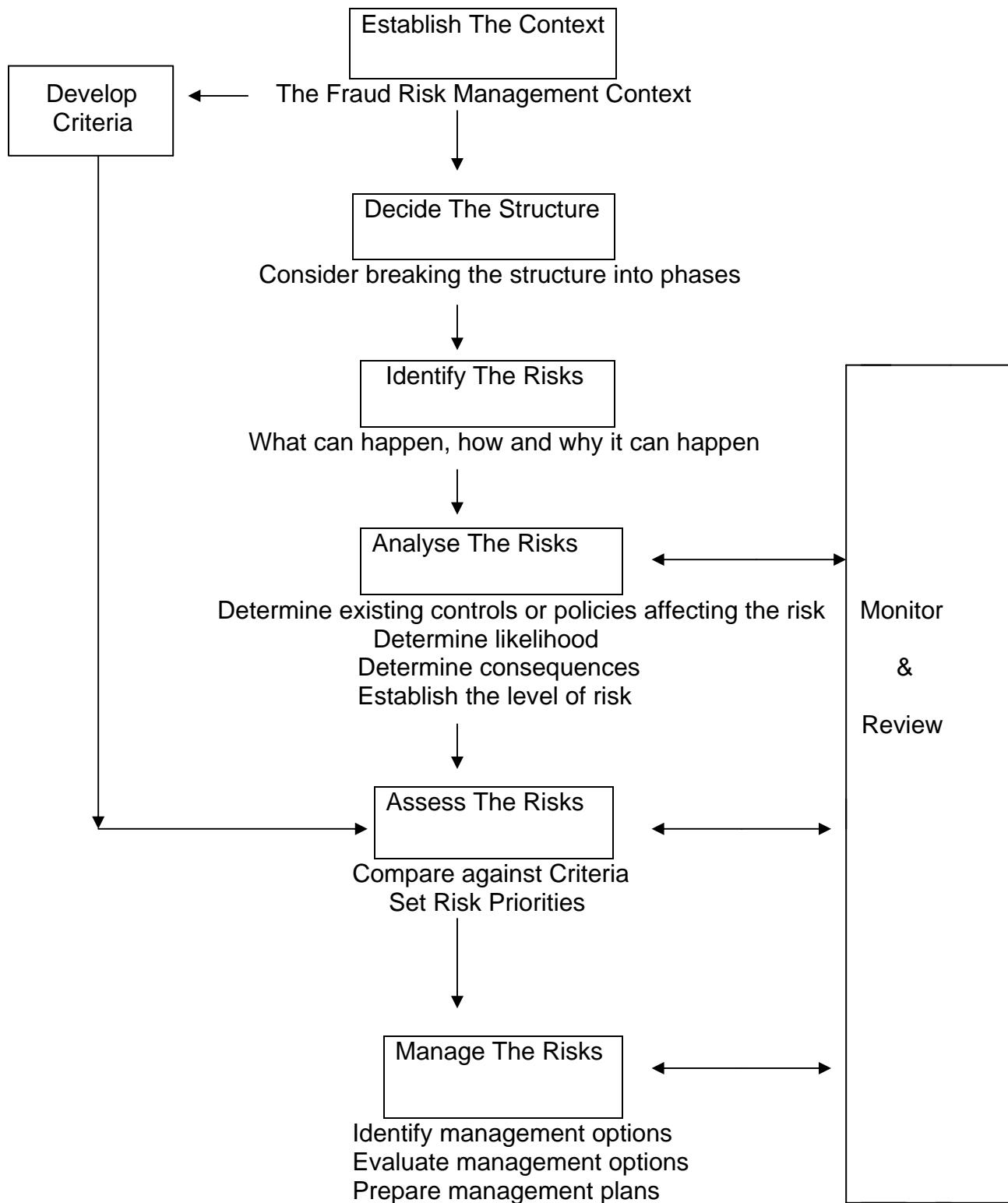
**Endorsements:** Senior Management

Peter Lynch.....Date: 21/05/2010

Review date: 21/05/2011



## Fraud Risk Management Process



# **The Fraud Risk Management Process**

(below are the main elements to the fraud risk management process)

## **1. Identification of Key Personnel**

Senior Management may appoint a member of management or other suitably qualified person with the responsibility of ensuring that:

The fraud risk management system is established and maintained in accordance with the organisation's policy and the effectiveness of the fraud risk management system is reported to the organisation's senior management. The people assigned to implement the fraud risk management policy have the authority to:

- a. Initiate action to prevent or reduce the adverse effects of risk.
- b. Control further management of fraud risks until the level of the fraud risk becomes acceptable.
- c. Identify and record any problems relating to the management of fraud risk.
- d. Initiate recommend or provide solutions through development of fraud management action plans.
- e. Review the fraud risks specific to certain fraud management plans as a whole & report to senior management regularly.

## **2. Establish the Fraud Risk Management Context**

The strategic context is the identification of fraud risks and their subsequent management for the prevention of dishonesty, adverse affects to profitability, including poor shrinkage control, waste control, theft and damage to the company by any form of deceit or malice.

## **3. Identify the Key Players**

There is a need to focus on the environment which the organisation functions in and to determine the crucial elements which support or impair the organisation's objectives. Also we must look at its ability to manage the risks within its framework associated with shrinkage, WOHS, misappropriation, waste and any type of deceit associated within the organisation. The key players must be identified within the fraud risk management environment, (the customers, staff, investors, contractors and competitors).

Determination of the relationship between the organisation and its environment is essential with respect to the organisation's operations policies arrangements by identifying the organisation's strengths, weaknesses, opportunities and threats. The environment includes competitive, financial, operational, public perception, customer, investors, cultural and legal aspects of the organisation's functions.

#### **4. Setting the Risk Criteria**

To set the risk criteria you must first determine the criteria against which risk is going to be evaluated; you must consider that the purpose of the process is to determine risks to integrity. Risk measurement can be developed when all the risk criteria are identified.

#### **5. Identifying Risks**

The objective of this phase is to develop a register of all possible risks for analysis. All risks should be included whether or not under the control of the organisation. Investigators familiar with the organisation would be suitable for this process although senior management could be utilised with a checklist approach in identifying the fraud risks.

After identifying a list of events it is necessary to consider possible causes and scenarios in any case an event can be identified which may initiate a risk.

#### **6. Analysing Risks**

In revealing the risks and causes, the fraud risk analysis is then primarily interested with determining the controls if any. Surrounding the issues identified as risk, the likelihood and consequences of something going wrong in terms of those controls. The analyses should consider how likely an event will happen, what the potential consequences are their magnitude and the potential of existing controls, if any.

A preliminary risk analysis can be carried out so that similar or low impact risks are excluded from the detailed study. These risks shall where possible should be listed to show the completeness of the risk analysis.

#### **7. Assess & Prioritise the Fraud Risks**

The assessment aims at determining the probability of the risk and whether the risk is high, medium or low, whether it is an acceptable risk or not. The output of the risk assessment is a prioritised list of risks for further action.

Low and accepted risks should be monitored and reviewed to ensure they remain at an acceptable level. If the risks do not fall into an acceptable level they should be managed and strategies put in place for control of the situation as soon as possible.

Strategies should be put into place to combat the fraud risks on the basis of what is the most appropriate and balanced against the cost of implementing the strategy and the extent of the benefits or opportunities created as a result of implementation.

## **8. Managing the Risks**

A management plan will require development to manage the medium to high risks whereas the low risks will be accepted but monitored. Consideration should be given to the following.

Avoiding or eliminating the risk or deciding not to continue with the activity may create risk. Risk avoidance can occur inappropriately because of an attitude of risk aversion; inappropriate risk avoidance may increase the significance of other risks.

Risk aversion results in, decisions to avoid or ignore risks regardless of the information available and costs occurred in treating those risks; failure to respond to risks; leaving critical decisions about intervention to other parties; deferring decisions or selecting inappropriate options.

Accept the risk of the organisation and establish appropriate risk financing plans. Reduce the likelihood of the occurrence and consequences by control, which may involve effectiveness policies, procedures or physical changes.

Transference of the risk by sharing the risk through subcontracting or insurance arrangements will reduce the risk for the organisation but may not diminish the overall risk for society as a whole.

Risks can be retained, those risks that have been treated sometimes have residual risk, and plans need to be put into place to control the residual risk which may involve risk financing.

## **9. Evaluate the Fraud Risk Management Options**

Selection of the most appropriate risk treatment option involves selecting and implementing the process which involves balancing the costs against the benefits derived from it. The cost of managing risks needs to be adequate for the benefits obtained.

When large risk reduction can be achieved with low expenditure such options should be implemented. The adverse effects of risk should be made as low as possibly practical, irrespective of any absolute criteria.

If the level of risk is high but taking the risk can see opportunities, then assessment of the risk needs to be based on the assessment of the costs of the risk treatment. The costs of rectifying the potential consequences versus the opportunities afforded by taking the risk.

## **10 Fraud Risk Management Plans**

With regard to the chosen treatment option for the risk should indicate how the particular plan is to be implemented. It should identify responsibility schedules and expected outcome of the intervention, budgeting, performance measures and the review process.

The responsibility for implementation of the fraud risk management plan should be given to those who are best able to control the risk and should be agreed on at the time of making the plan.

## **11 Linkage to other Governance Processes**

Governance processes linked to fraud and corruption control are issues that need to be addressed by large organisations. A fraud and corruption strategy should be introduced with consideration of the suite of governance issues which impact directly upon the organisation being, physical security, computer & information security, internal audit, ethics & business risk management.

It is important for linkages to be wherever possible, to these other processes. These linkages will have a front end risk management plan with risk registers, focus groups and questionnaires.

Fraud and corruption control cannot rely solely on multipurpose risk management plans; there are implications for dealing with fraud and corruption prevention together.

One implication is that risk treatments for fraud are going to tend towards dealing with financial and information systems compared to risk treatments for corruption issues are going to tend towards changing the organisation's culture.

Mechanisms for enhancing ethics are communication of a high level of ethical values and code of conduct with setting out of clear policies for the acceptance of gifts and avoidance of conflicts of interest. Senior management walking the talk facing issues with its stated ethical values also enhances ethics.

Although it is not said that risk management has nothing to offer in the governance process, it can perform a valuable role in analysing the adequacy of this group of governance processes and point to deficiencies either in the structure or implementation.

## **12. Procedures for Reporting Fraud & Corruption**

It is important that all instances of fraud and corruption detected within or against the organisation are reported to senior management. It is important that all persons within the framework of the organisation have alternative means of reporting matters of concern involving allegations of unethical or illegal activities.

Employees and others must have avenues in which they can direct their concerns, being allegations or suspicions to the senior management of the organisation.

Reporting of activities involving fraud or corruption needs to be able to be communicated to senior management through the normal reporting channels, outside the normal reporting channels but within the entity and through reporting channels external to the organisation.

The objective of the alternative reporting mechanisms is to ensure that all factual or potential fraud and corruption control system failures are corrected in an appropriate way.

The systemic and recurring problems of non compliance need reporting to those with the sufficient authority to correct them.

Internal and external reporting arrangements should be utilised in a fraud and corruption control program.

### **13. Procedures for Handling Allegations.**

All allegations should be dealt with quickly and decisively and the disclosure of information in relation to the allegations should be strictly limited, reasons are suspects are likely to destroy evidence that could assist in the judgement of a case.

Extensive knowledge of a case could damage the reputation of a suspect before a formal judgement has been made. The privacy of the suspect other staff members and organisational clients could be compromised.

Organisational procedures should be established so that all internal cases are treated on a need to know basis, staff that become knowledgeable about an active case in which they are not working on or involved with should be encouraged not to discuss the information with anybody.

When a report of fraud is first received, it should be referred in confidence to the organisation's department that is responsible for handling the allegations. There should be obligations in handling the allegations but the options for action are if it is without foundation it can be dismissed as trivial, mischievous or vexatious. If it is of a disciplinary nature it should be dealt with in accordance with internal disciplinary procedures.

The report of fraud may be resolved by the application of administrative or civil action to recover losses or if the fraud is of a serious criminal nature it warrants investigating as a serious criminal matter.

Reaching a decision about what action should be taken about a particular case, a senior officer of the organisation should consider the likelihood of a successful conclusion recognising those cases of a criminal nature, the decision about what action is taken is made by the DPP.

#### **14. Procedures for Investigating Cases**

In investigations anonymous information must be treated with utmost skepticism until its veracity is confirmed by independent investigations.

A more complete investigation should only proceed if the information received from the anonymous sources is appropriately supported by evidence.

Appropriately skilled personnel who are independent of the business unit being examined should only conduct an investigation.

The independent party can be an external law enforcement agency or a manager or senior person within the entity itself or an external consultant operating under the supervision of an independent senior person from within the entity.

External parties engaged in the conduct of investigations should be appropriately qualified and have relevant experience. The investigation should be managed with best practices within the respective jurisdiction and the investigating officer should be an acceptable person within the jurisdiction in which the investigation is being conducted.

External parties engaged to assist in investigations on the entity's behalf should be required to enter into a binding agreement in relation to the release of confidential information coming into possession of the person or persons during the investigation. External consultants need to have expertise when conducting investigations.

Investigations and resulting disciplinary proceedings should be conducted in an atmosphere of transparency at all times ensuring the rules of justice are observed.

The guiding principles of the investigation into alleged or improper conduct should be independent and objective. Investigations should comply with all relevant legislation within the jurisdiction in which the action will or could be initiated.

Records of the investigations should be kept on file and kept in accordance with the best policy legal guidelines.

An entity conducting an investigation into allegations of misconduct should ensure that the information arising from or relevant to the investigations should

not be disseminated to anyone other than those directly responsible for and which holds a position within the investigation case and department involved.

Investigations will involve the following investigative activities:

- a. Interview of relevant witnesses, obtaining statements, where appropriate including witnesses internal and external of the entity.
- b. Review and collating of the documentary evidence.
- c. Forensic examination of computer systems.
- d. Examining telephone records.
- e. Inquiries with financial institutions (court orders required).
- f. Inquiries with other third parties.
- g. Data search and seizure.
- h. Expert witness and specialist testimony.
- i. Tracing funds/assets/goods.
- j. Preparing briefs of evidence.
- k. Liaison with the police or other law enforcement or regulator agencies.
- l. Interview persons expected of involvement in fraud and corruption.
- m. Report preparation.

Investigations into improper conduct within an entity should be subject to an appropriate level of supervision by a responsible committee within the entity having regard to the seriousness of the matter under investigation. In serious cases it is contemplated that the relevant committee will be the audit committee, the ethics committee or the board of directors.

## **15. Procedures for Collecting Information**

In dealing with fraud and corruption threats it is essential that all previous breaches have been recorded. The organisation should have on hand and maintain a management information system that records:

- a. All instances of fraud & corruption.
- b. Losses to the organisation or potential for damage to the reputation of the organisation.
- c. Investigative action taken.
- d. Disciplinary action taken or outcomes of matters which have been prosecuted and any changes to procedures and practices arising from the incident.

The process of collecting and storing of information in the fraud and corruption information collection allows for the publication of an annual report for review of parliament in the public sector. This and assure parliament and through them, the community that these issues are being handled professionally in the organisation.

## **16. Awareness Raising and Training**

Fraud and corruption awareness is a necessity for the overall process of fraud and corruption prevention. Fraud and corruption control officers have a duty from the relationship with the entity and the public interest.

The fraud and corruption activities include fraud and corruption issues in induction training, running specific awareness programs for all staff, discussion of issues in staff newsletters and senior officers being made responsible for fraud and corruption in their performance agreements.

Implementation of the competency standards for all senior fraud and corruption controllers and fraud and corruption officers has become mandatory. Within government agencies although some fraud and corruption awareness and training qualifications from universities like Charles Sturt University may be utilised where desired. A set of competency standards has been articulated as part of the Public Sector Training Package (PSTP). The courses based upon these standards are:

Certificate 4 in Government (Fraud Control Investigations);  
Certificate 4 in Government (Fraud Control Prevention/ Detection);  
Diploma in Government (Fraud Control Investigations);  
Diploma Government (Fraud Control Prevention/Detection); and  
Advanced Diploma in Government (Fraud Control Management).

The competency standards have been introduced to raise the level of professionalism in the area of fraud and corruption control.

## **17. Procedures for Evaluating Success of the Strategy**

At least every twelve months, all business units (or at least all business units with an apparent disposition to fraud) should ensure that strategies developed during the most recent fraud risk assessment are reviewed for effectiveness and amended where necessary.

The Fraud Control Officer should be allocated responsibility for co-coordinating compliance with the twelve monthly reviews of fraud mitigation strategies in addition to the biennial fraud risk assessment.

## Bibliography

Australian Institute of Criminology, *Situational Crime Prevention, Research & Public Policy Series*, Australian Institute of Criminology, Canberra.

Boardman, C & Klum, V 2001, Building Organisational Integrity, in *Corruption & Anti Corruption*, P Larmour & N Wolanin (eds), Asia Pacific Press, Canberra.

Bluck, P 2002, *Band-Aids for Amputees: Whistleblowing in the Commonwealth*, Aial Forum, no.33, pp.22-29.

Elliston, F, Keenan, J, Lockhart, P & Schaick J 1985, *Whistleblowing Research: Methodological and Moral Issues*, Praeger Publishers, NY USA.

HM Treasury 2003, *Managing the Risk of Fraud: A Guide for Managers*, HM Treasury.

Independent Commission against Corruption 2002, *Fighting Fraud: Guidelines for State and Local Government*.

Keelty, M 2001, *Fraud Control and the Commonwealth: Corporate Risk*, Corporate Risk Magazine: Australian Federal Police, pp30-32.

Near, JP & Miceli, MP 1985, Organisational dissidence: The case of whistleblowing, *Journal of Business Ethics*, vol.64, no.3, pp.322-347.

NSW Department of State and Regional Development 2000, *Business Fraud*, no.2 Business Enterprise Centre, NSW.

Roberts, P 2003, *Fraud Prevention*, Faculty of Arts Study Guide JST412, Charles Sturt University, Albury-Bathurst-Wagga Wagga NSW Australia.

South Australian Government, *Fraud Risk Management Policy & Procedures* series no.2, Human Resource Management Division, Department of The Premier and Cabinet, SA.

Standards Australia International 2003, *Fraud and Corruption Control*, Australian Standard AS8001, Council of Standards Australia Sydney.

Standard Association of Australia 1999, *Risk Management*, Australian/New Zealand Standard AS/NZ4360 Council of Standards Australia, Sydney.

Victoria Auditor General's Office 2000, *Fraud Prevention Strategies*, Level 14, 222 Exhibition St Melbourne.