

## **CORRUPTION IN THE WORKPLACE**

**How to prevent it**

•

**How to detect it**

•

**What to do about it**

**Criminal Justice Commission**

© Criminal Justice Commission 1993

Apart from any fair dealing for the purpose of private study, research, criticism, or review, as permitted under the Copyright Act, no part of this document may be reproduced by any process without permission. Inquiries should be made to the publisher, Criminal Justice Commission (Queensland).

ISBN 0-7242-5642-3

Criminal Justice Commission  
557 Coronation Drive  
Toowong, Queensland

Postal PO Box 137  
Address: Albert Street  
Brisbane 4002

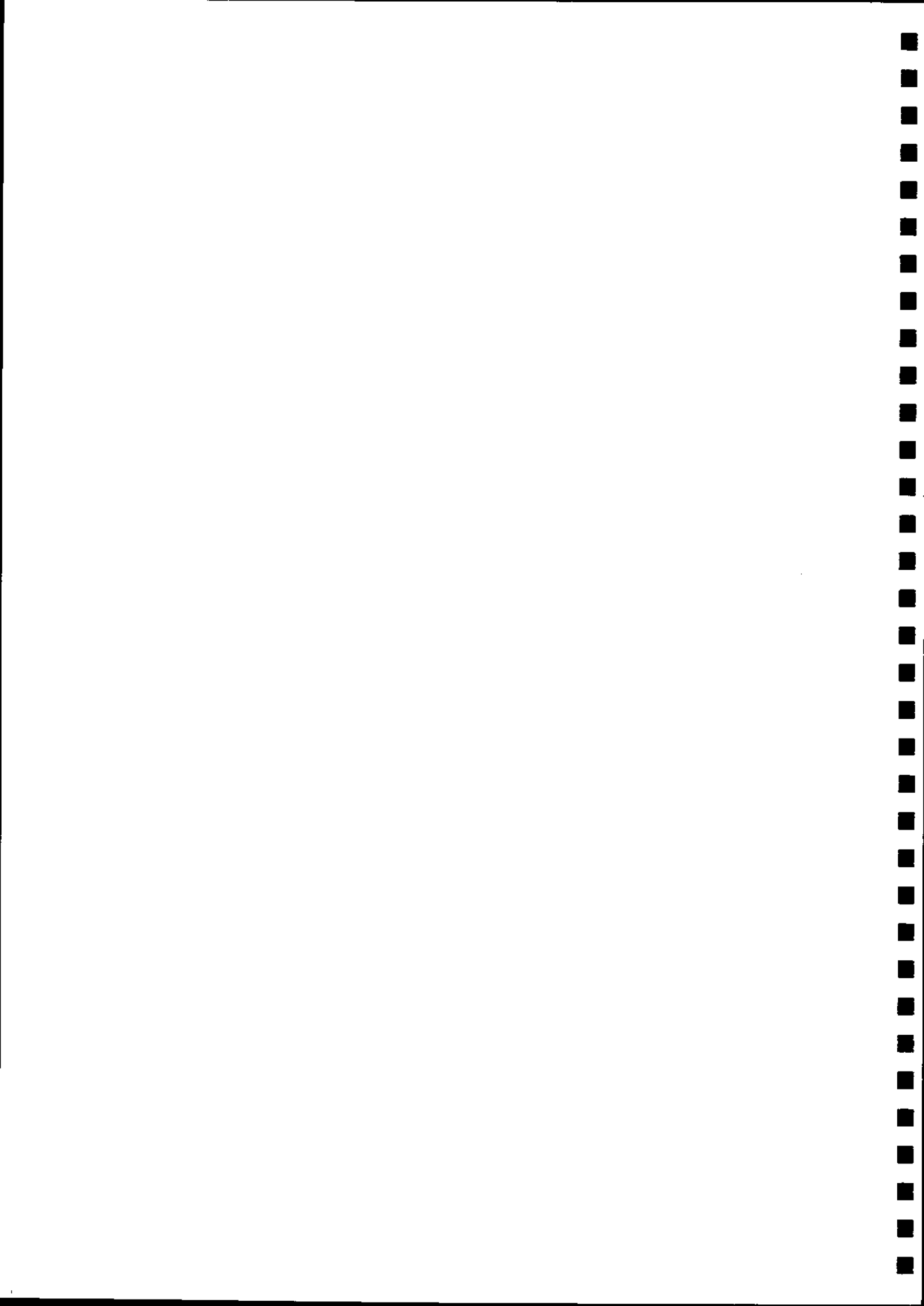
Telephone: (07) 360 6060  
Facsimile: (07) 360 6333

## ACKNOWLEDGMENTS

The major contributor to this manual was Barry Leithhead, a consultant in risk analysis and internal auditing. Other contributors were Dr Noel Preston and Dr Trevor Jordan of the Bureau of Ethics and Human Change at the Queensland University of Technology; Robert McDonald, President of the Queensland Board of the Institute of Internal Auditors Australia, who contributed with the permission of the Department of Primary Industries; Robert Renew, former President of the Queensland branch of the Australian Society of Practising Accountants, who gave a private sector perspective; and Robert Hailstone, Director, Corruption Prevention Division, Criminal Justice Commission.

Acknowledgments are also due to : American Society for Public Administration for material from *Combating Corruption : Encouraging Ethics* by W L Richter 1990; Anderson Publishing for material from *Lying, Cheating and Stealing* by Gwynn Nettler 1982; Canberra Bulletin of Public Administration for material from 'Fraud in Government – A Criminological Overview' by Dennis Challenger 1988; Kluwer Academic Publishers for material from 'Danger Signs of Unethical Behaviour' by Robert Cooke 1991; John Wiley for material from *Fraud Auditing and Forensic Accounting* by Jack Bologna and Robert Lindquist 1987.

Front cover: newspaper clippings, courtesy of *The Courier-Mail*.



ACKNOWLEDGMENTS	iii
-----------------	-----

FOREWARD	ix
----------	----

1.	INTRODUCTION	1
1.1	How extensive is corruption?	1
1.2	Five corruption myths	1
2.	WHAT IS CORRUPTION PREVENTION?	2
2.1	What is risk assessment?	2
3.	ETHICS AND CORRUPTION	2
3.1	Why be concerned about ethics?	3
3.2	What are ethics?	3
3.3	Ethical principles	4
3.4	Professionalism and public sector ethics	4
3.5	Are public sector ethics different?	4
3.6	Are there fundamental ethical obligations for public officials?	5
3.7	What about 'the public interest'?	5
3.8	What is the role of rule and regulation in ethics?	5
3.9	Building an ethical organisation	6
3.10	Ethics at risk	6
3.11	Adopting an ethical code to prevent corruption	7
3.12	In conclusion	7
4.	THE NATURE OF CORRUPTION	8
4.1	What is corruption?	8
4.2	Official misconduct	8
4.3	Management responsibility for corruption prevention	9
4.3.1	Prevention	9
4.3.2	Detection	9
4.3.3	Notification	9
4.3.4	Prosecution	9
4.4	Potential corruption sources	10
4.4.1	Managers	10
4.4.2	Staff	10
4.4.3	Clients	10
4.4.4	Suppliers and contractors	10
4.4.5	Other parties	10
4.5	Corruption categories	13
4.6	Allegations received by the CJC	13
4.7	Typical corruption symptoms (red flags)	13
4.7.1	Staff	13
4.7.2	Transactions	14
4.7.3	Documentation	14
4.7.4	Audit	15
4.8	A selection of incidents	15
4.9	Corruption in local government authorities	16
4.9.1	Case A	16
4.9.2	Case B	16
4.9.3	Case C	17
4.9.4	Case D	17
4.9.5	Case E	17
4.9.6	Case F	17
4.10	Discussion of local government case studies	17

5.	PREPARING FOR CORRUPTION PREVENTION	18
5.1	Corruption control concerns everyone	18
5.2	Whistleblowers	18
5.3	Individual rights in investigations	18
5.4	Corruption prevention models	19
5.4.1	Who might be tempted to be corrupt?	19
5.4.2	Why people lie, cheat and steal at work	20
5.4.3	Characteristics of corrupt people	21
5.5	Management accountability	21
5.6	Corruption prevention is better than cure	21
5.7	High risks areas are easier to predict	21
5.7.1	Theft	21
5.7.2	Wrong supply	22
5.7.3	Malicious damage	22
5.7.4	Bribery	22
5.7.5	Undue influence and power	22
5.7.6	Neglect of duty	22
5.7.7	Unauthorised actions	22
5.7.8	Misuse of resources	23
5.7.9	Invalid information	23
5.7.10	Forgery	23
5.8	Developing a corruption prevention policy	23
5.9	The corruption prevention plan	23
5.9.1	Relationship to other plans	23
5.9.2	Contents of a corruption prevention plan	24
5.10	A corruption prevention strategy	24
5.11	Corruption prevention officers	24
5.12	The corruption prevention staff register	24
6.	ANALYSING THE FINANCIAL CORRUPTION RISKS	25
6.1	Revenue risks	25
6.2	Expenditure risks	28
6.3	Resources risks	31
6.3.1	Assets	31
6.3.2	Financial resources	31
6.3.3	Human resources	31
6.3.4	Information resources	31
6.4	Assets risks	36
6.5	Risks for liabilities and obligations	36
6.6	Summary	36
7.	THE RISK PROFILE	39
7.1	Known corruption incidents	39
7.2	Organisational objectives	39
8.	ASSESSING CORRUPTION RISKS	51
8.1	Ranking the assessment of corruption risks	51
8.2	Assessment of high corruption risks	51
8.2.1	Incentive	51
8.2.2	Opportunity	51
8.2.3	Concealment	52
8.2.4	Prevention difficulty	52
8.2.5	Detection difficulty	52
8.2.6	Diminished ethics	52
9.	A SIMPLIFIED RISK ANALYSIS PROCEDURE	55
9.1	The key players and their roles	55
9.2	The model	55
9.3	Scope	55

9.4	Identification	55
9.5	Evaluation	55
9.6	Control	56
10.	DETAILED RISK ANALYSIS PROCEDURES	59
10.1	Summary analyses	59
10.2	Comparative ranking	69
10.3	Questionnaire-based methods	69
11.	CORRUPTION PREVENTION AND CONTROL PRACTICES	70
11.1	Corporate ethos and practice	70
11.2	Management attitude	70
11.3	Staff involvement	71
11.4	Key control elements	71
11.4.1	Effective supervision	71
11.4.2	Adequate authorisation procedures	71
11.4.3	Segregating conflicting duties	71
11.4.4	Safeguards against conflicts of interest	72
11.4.5	Well-defined transaction procedures	72
11.4.6	Data and management information systems security	72
11.4.7	Physical security over assets	72
11.4.8	Independent review of controls	72
11.5	Analysis of controls	72
12.	DESIGN AND EVALUATION OF CORRUPTION PREVENTION CONTROLS	74
12.1	Can there be too much control?	76
12.2	Overcoming resistance to controls	76
12.3	Implementing controls	76
12.3.1	Physical security of assets	77
12.3.2	Confidential information	79
12.3.3	Purchasing	79
12.3.4	Contracts	81
12.3.5	The contract register	81
12.3.6	Contract quotation evaluation	81
12.3.7	Travel allowances and expenses	82
12.3.8	Levy-based income	82
12.3.9	Licensing and registration	82
12.3.10	Benefits and grants	83
12.3.11	Management information systems	83
12.3.12	System resources and prevention controls	83
13.	WHAT HAPPENS WHEN CORRUPTION IS DETECTED?	84
13.1	Reporting to the CJC	84
13.2	CJC investigations	84
13.3	CJC contact with you	85
13.4	Management systems review	85
	BIBLIOGRAPHY	87
	APPENDIX 1 - ADDITIONAL RESOURCES	89
	APPENDIX 2 - QUEENSLAND PUBLIC FINANCE STANDARDS	91
	APPENDIX 3 - STATEMENT OF AUDITING PRACTICE AUP 12	97
	APPENDIX 4 - STATEMENT OF AUDITING PRACTICE AUP 16	103





The Criminal Justice Commission (CJC) was established in November 1989, under the *Criminal Justice Act* 1989, in response to the recommendations of the Commission of Enquiry conducted by G E Fitzgerald QC. The CJC is charged with

- investigating all complaints of, and information concerning, alleged or suspected corruption by members of the Queensland Police Service (QPS) and official misconduct by persons holding appointment in units of public administration
- hearing and determining disciplinary charges of official misconduct through its Misconduct Tribunals
- investigating and taking measures to combat organised and major crime
- informing the Legislative Assembly about these activities.

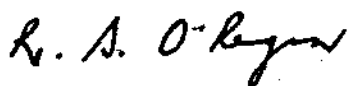
The CJC has developed considerable expertise in the fight against corruption in the public sector. It

- conducts research and enhance public, parliamentary and forensic awareness of the issues confronting the administration of criminal justice in Queensland
- exposes corruption and official misconduct through hearings and reports to Parliament
- provides evidence to the courts, Misconduct Tribunals or other disciplinary proceedings which leads to the appropriate action against persons engaged in corruption or misconduct (including official misconduct)
- actively seeks to reduce the incidence of misconduct and official misconduct in the QPS and official misconduct in units of public administration.

To achieve these goals the CJC offers and renders assistance 'by way of education and liaison, to law enforcement agencies, units of public administration, companies and institutions, auditors and other persons concerned with the detection and prevention of corruption of official misconduct' (s. 2.20(2)(f) of the *Criminal Justice Act* 1989).

Through its Corruption Prevention Division, the CJC assists government departments, local government authorities, the QPS and statutory authorities to develop proactive corruption prevention strategies by liaising, providing advice, and coordinating conferences, workshops and seminars.

The CJC works with primary, secondary and tertiary educators to raise awareness about public sector corruption. It also seeks to educate the public about these issues through the media, and contact with community-based organisations and professional bodies.



Mr Robin O'Regan QC  
Chairperson



# 1. INTRODUCTION

This manual is designed to help managers take a proactive approach to corruption control.

Corrupt activities can severely limit your organisation's ability to carry out its mission and to meet its performance objectives. Unheeded corruption also damages staff productivity and morale, which undercuts your organisation's image and the quality of service it can offer.

We offer this manual as a resource. It is the product of wide consultation with risk management consultants, the Institute of Internal Auditors, public service departments, universities, behavioural scientists and officers of the Commission.

The manual will help you develop sound practices to prevent and detect corruption. It explains how to

- recognise those staff who might be at risk
- identify system shortfalls and loopholes
- analyse and rank risks
- design, evaluate and improve controls
- develop strategies, policies, practices and resources to prevent and combat corruption.

## 1.1 How extensive is corruption?

The full extent of corruption in Australia is not known. The most successful frauds, for example, are never detected. Launching a Commonwealth inquiry into fraud on government in 1986 the Federal Special Minister of State, Mick Young, said 'Figures ranging from \$5 billion to as high as \$30 billion have been cited. These figures could be exaggerated. The simple fact is we don't know.'

Press advertisements placed Australia-wide in 1993 claimed that the figure was closer to \$10 billion.

The Queensland public sector annually manages about \$19 billion. In 1988 *The Courier-Mail* suggested that perhaps as much as \$88 million was being fraudulently misused. How this was estimated is unknown.

It has been suggested in Queensland that 20-30% of all third party claims were false or exaggerated (*The Sunday Mail*, 5 June 1988). An estimate of \$10,000 million insurance fraud would not seem to be an exaggeration. The real figure is not known.

Australia is not alone. In 1983 an American National Institute of Justice publication stated that

fraud in government benefit programs is now widely viewed to be a serious national problem. Estimates by the General Accounting Office suggest the problem may cost the public anywhere from \$2.5 billion to \$25 billion per year. (Gardiner et al 1982)

It is clear that public sector corruption and white collar crime costs Australia large amounts of money every year.

While fraud is a problem, it is only one form of corrupt behaviour. Another form, termed *official misconduct* in the *Criminal Justice Act*, includes lack of impartiality, breach of the community's trust and the unauthorised release of confidential information.

## 1.2 Five corruption myths

Deeply embedded in our culture are myths that make it harder to prevent corruption. These include:

1. *Fraud against government is a victimless crime and therefore is not really a crime at all.*

Terms such as "perks", "fiddles" and "rorts" describe minor, and sometimes not so minor, forms of corruption. They soften the nature of acts that often quite clearly involve criminal activity.

2. *It is un-Australian to do in a mate.*

This attitude undermines those who attempt to "keep the system honest". "Whistleblowers" may be victimised (see section 5.2).

3. *You can't beat City Hall.*

This suggests that the ordinary people cannot stand up to the might of a bureaucracy when they suspect corruption, or are victims of corrupt activity.

In 1992, 75% of public sector employees we surveyed said they felt powerless when confronted with corrupt activity by a superior.

4. *There is no corruption in my organisation.*

Senior executives may not wish to face the reality that corruption can and does take place under their administration.

5. *I won't get caught.*

This is a powerful incentive. Attitudes that motivate people to become corrupt are discussed in section 4.

useful for organisations with limited resources while the detailed one may be better for complex organisations. Both approaches have been trialled.

Risk assessment is a systematic **and** intuitive method of looking behind and beyond accounting procedures to determine

- weak links in a system of controls
- loopholes in a system that can be exploited
- how systems can be bypassed, allowing illegal activities to remain undetected
- the degree to which the organisational culture encourages corruption
- which staff members are at risk of being corrupted.

## 2. WHAT IS CORRUPTION PREVENTION?

Prevention focuses on patterns of conduct, unregulated access and opportunities to engage in unauthorised activities rather than on the accounting errors and omissions that financial auditors address.

Prevention requires visible management commitment to a code of conduct, staff training, effective supervision, timely checks and effective internal communication.

Poor management and lax controls create a favourable climate for corruption to flourish. Stress can lead honest staff to become dishonest. Developing an awareness of the signs of such behaviour is the first step in corruption prevention.

### 2.1 What is risk assessment?

It is not easy to pinpoint problem areas. Risk assessment detects shortfalls or loopholes in management, personnel and financial systems. There is no preferred model. Risk assessment analysis aims to anticipate losses.

The starting point is to learn from what we already know. Losses in one organisation may provide valuable lessons for others; identifying corruption in one area of an organisation may lead to detection of corruption in other areas.

In this manual we present both a simple and a detailed technique. The simple option could be

## 3. ETHICS AND CORRUPTION

This section discusses the relevance of ethics and ethical behaviour to corruption prevention because an organisation needs to be clear about ethics before it can deal effectively with corruption.

We consider the following issues:

- What are ethics?
- Why is ethics important to your organisation?
- What is the relationship between ethics and professionalism?
- What is involved in building an ethical organisation?
- How do codes of conduct and regulation express the ethics of an organisation?

We assume that

- ethical failure and ethical achievement can be attributed to both individual behaviour and to the organisational culture

- corruption prevention should address both institutional and personal issues
- ethical behaviour can be learned
- ethics can be taught through modelling or example (a senior official who cares for staff and who is scrupulously honest will be likely to foster integrity)
- training programs in ethics are developed not only to alert staff to behaviour that should be avoided but also to help them develop skills in moral reasoning on the job.

### 3.1 Why be concerned about ethics?

Technological advances have created a situation in which our ability to determine what we *can* do has outstripped our capacity to decide what we *ought* to do.

Ethical issues pervade our lives. We are faced with moral issues in medicine, science and technology. We realise that certain developed nations are acting without ethical concern for the environment, allowing technology and economics to be the primary basis for decisions.

The Fitzgerald Report emphasised the importance of ethics for the public sector. Other professionals have been paying attention to ethical questions by instituting organisational codes of conduct and by running conferences on ethics.

In an unethical climate, corruption is likely to increase; conversely, when ethical behaviour is encouraged, corruption is likely to decline.

It is probably no accident that, during the 1980s, corporate and professional law-breaking (among business executives and their financial and legal advisers) increased when the community was paying little attention to ethics and when "looking after number one" was the only guiding principle. To many, it seemed that, in business, as elsewhere, "greed was good".

Recent history, however, has shown that when an organisation lowers its ethical standards there is also likely to be a decline in strict adherence to the law. Acting unethically may not be illegal, but it creates a climate in which illegal behaviour becomes more easily accepted.

Codes and practices have limited effect unless the ethical principles which they promote are understood and accepted.

An effective ethical strategy should deal with administrative, economic and legal issues. It must also focus on rights, responsibilities, equity, honesty, freedom and justice. An understanding of ethical reasoning helps to identify and to deal with the changing forms of corruption.

Before it was made illegal, corruption would have been seen to be unethical. We need to think about the ethical implications of future developments and activities that might be outside present laws and regulatory codes.

Ethical behaviour extends beyond the mere adherence to a set of rules. There is often scope for unethical behaviour while working strictly within the rules.

### 3.2 What are ethics?

*Ethical* and *moral* behaviour is socially and culturally accepted to be right or good. *Unethical* and *immoral* behaviour is accepted to be wrong or bad.

Ethics is also used to describe the rules or standards governing the conduct of members of a profession. The requirements of a particular job or professional practice introduce further possibilities for evaluating what is right and wrong.

Ethical issues in the public sector can be problematic because staff may be confronted with choosing a course of action from several possible alternatives, each of which has merit.

The problem is worse when we are aware of conflicts between the differing ethical levels on which we conduct our lives. We operate via

- personal codes of morality or ethics
- professional ethics
- organisational ethics
- social ethics.

Some people need guidance to develop a sense of moral autonomy. They may fear that discussing their personal ethics may subject them to scrutiny by their colleagues. It must be made clear that personal ethics are relevant only when they impinge upon work.

How would we describe the morally educated person? Such a person

- cares for others
- has self-esteem
- values social justice
- is democratic
- respects the environment
- is honest
- is open
- values and strives for excellence
- is loyal.

An ethical society values justice, equality, freedom, and diversity.

### 3.3 Ethical principles

The principles that apply to judgments about whether actions are good or bad are discussed below.

The ethical merit of an act can be judged according to its *consequences*. Before making a decision, public officials need to consider the consequences for all who are affected. This can often be rather difficult.

Consider the following:

What should an individual do if offered tickets to a sporting event by a company that does business with the organisation?

Is the acceptance of such an invitation likely to influence decisions or behaviour in respect to the donor company?

If there were to be an influence, it would be unfair to that company's competitors. If a decision must be made to select from among several companies, the decision must be made out of a sense of obligation to the donor company rather than be based on the facts.

Even if there is no apparent influence, questions must be asked about the likelihood of the individual's reputation for objectivity being damaged if the issue becomes public. (Richter 1990)

If the organisation concerned has no policy dealing with the acceptance of gifts, the person who was approached should seek clarification from management. This is because individuals are not always able to calculate the consequences of their actions. When similar questions crop up repeatedly, the ethical principles involved should be placed in a code of conduct that stipulates the kind of behaviour we expect from all staff in such circumstances.

However, blind obedience to rules will not always serve us well. For example, while honesty is important, few people would hesitate to lie if it meant that an innocent life would be saved. Principles need to be ordered in some way so that we understand which principle should override another in certain circumstances.

### 3.4 Professionalism and public sector ethics

Professional people have special powers and responsibilities. For example, police officers must learn standards of behaviour appropriate to the possession of firearms. They must be aware of the ethical dilemmas that may arise from their use of firearms.

While most staff in the public sector do not have to use guns, they do have access to important resources, which they must use responsibly. They also need to consider the consequences of their actions.

Honesty and integrity are important for everyone, but managers have a particular responsibility to establish and maintain ethical practices for the prevention and detection of corruption. Officials must be impartial and fair, maintain confidentiality and refrain from abusing their powers.

On occasion there are conflicts between professional ethics and one's duty. A duty of care for a client may clash with responsibilities for the public interest. These cases can prove difficult. Senior managers should anticipate situations of possible conflict, and set up mechanisms to resolve clashes of obligations.

### 3.5 Are public sector ethics different?

Public sector ethics have characteristics not found elsewhere. Public sector workers are often close to those who wield political power. This can mean

being presented with hard choices and having to seek compromises that are the "lesser of two evils". We often ask to what extent we should be cast as a "moral actor" in our work setting. Should a medical doctor lie to a dying patient about prospects of recovery? Should a lawyer maintain confidentiality if it puts another person at risk? A public sector professional can legitimately ask 'What right do I have to exercise ethical judgment at all?' There is no easy escape from moral decisions.

It is a mistake, however, to treat the public sector as if it were homogenous. Fraud and risk management for health care workers, for example, might differ markedly from those in emergency services or transport.

### 3.6 Are there fundamental ethical obligations for public officials?

The Electoral and Administrative Review Commission *Report on Codes of Conduct for Public Officials* suggests five fundamental obligations:

1. **Respect for the Law and the System of Government** – public officials shall uphold the laws of Queensland and Australia, and shall implement the decisions and policies of the Government, and shall not, without just cause, be a party to their breach, evasion, or subversion.
2. **Respect for Persons** – public officials shall treat members of the public and other officials honestly and fairly, and with proper regard for their rights, entitlements, duties and obligations, and shall at all times act responsively in the performance of official duties.
3. **Integrity** – public officials shall at all times seek to maintain or enhance public confidence in the integrity of public sector administration, and to advance the common good of the community which they serve, in recognition that public office involves a public trust. In particular, officials shall ensure that their official powers and position are not used improperly for personal advantage, and that any conflict between personal interests and official duty that may arise is resolved in favour of the public interest.

4. **Diligence** – public officials shall exercise due diligence, care and attention, and always seek to achieve high standards of public administration in relation to the duties and responsibilities of their official position.

5. **Economy and Efficiency** – public officials shall avoid waste, abuse and extravagance in the provision or use of public resources, and shall expose fraud and corruption of which the official is aware.

### 3.7 What about 'the public interest'?

In a democratic society the public interest must go beyond private and political interests but it should not unnecessarily interfere with private interests. The political process ultimately arbitrates and declares what the public interest, or the good for society, might be.

*Public trust* is a basic element in public sector ethics. In 1829 the American Henry Clay gave this definition:

Government is a trust, and the officers of government are the trustees and both the trust and the trustees are created for the benefit of the people.

From the notion of public trust comes two obligations:

- the affirmative duty to pursue the public interest
- the obligation to refrain from conduct that uses public office for private benefit or partisan advantage.

Many cases of official corruption are clear instances of the abrogation of this trust and the pursuit of private interest over the public interest.

### 3.8 What is the role of rule and regulation in ethics?

Some public officials feel that mere technical compliance with written ethical standards protects the public. However, this establishes an ethos that will inevitably result in more rules and less personal responsibility for decisions about what is right and wrong.

This approach is close to bending the rules or finding loopholes which will in turn create a demand for tightening the rules. A cycle of regulating for morality will continue.

Yet providing a set of procedural guidelines ensures that people know the constraints operating upon them, and encourages even those individuals whose moral capacities are limited to comply. It also gives the whistleblower a framework by which to judge what is unacceptable behaviour.

### 3.9 Building an ethical organisation

There are three types of organisational structures that can profoundly affect accountability to the public.

In *hierarchical* organisations, social relationships, roles and responsibilities are often clearly distinguished. Accountability is primarily to immediate superiors and therefore only indirectly to the public. This structure encourages rules and regulations. Decision-making relationships are narrow rather than broad-based. Corruption is seen as something that others (the "bad apples") do and the view is that offenders deserve punishment.

Paradoxically, it is sometimes easy for the corrupt to find a niche in such a rigid hierarchy. It may be difficult for staff to question the decisions or actions of their superiors.

In *loyalty-based* organisations, relationships are founded on a sense of belonging to a group. Decision-making is biased to favour sustaining group relationships rather than observing the letter of the law. People are liable to ignore the faults and shortcomings of members of their group.

Group members may be harsh and legalistic towards outsiders, for example, clients or officers in other departments. Corruption may take place as a disproportionate flow of goods or rewards out of the organisation to the in-group. Group loyalties prevent the flow of disapproving opinion and information about the activity back to the organisation.

In the *web* or *network-based* organisation, individuals at various levels of authority and expertise are seen, quite genuinely, to be working together towards common goals. The emphasis is no longer on us versus them. Whenever appropriate, all parties within and without the organisation are consulted, informed or involved in decision-making.

Within such an organisation, accountability is not a matter of surveillance but of openness so that there is no secrecy about any organisational matter. Beyond the organisation, the social relationships address the vital need for the public to be kept well-informed through processes of genuine interaction and discussion.

Consider the advantages to be gained from adopting the web or network-based model in your organisation.

### 3.10 Ethics at risk

An American authority on business ethics, Robert Cooke (1991), has identified 'red flags' that can help indicate if an organisation is at ethical risk:

1. *It emphasises short-term goals above long-term considerations.*

Solutions to ethical dilemmas require long-range commitments. They should not merely focus on the next budget estimate or the next quarter's earnings.

2. *It routinely ignores or violates its code of ethics.*

Ethical standards must be soundly integrated into the corporate culture. Regular monitoring should include formal counselling or warnings or dismissal for those who fail to comply.

3. *It is satisfied with "quick fixes" to ethical problems at risk.*

Complex problems require thoughtful analysis.

4. *It puts costs above ethical standards.*

Short-term gains are usually undercut by corrupt activity over the long term.

5. *It visibly discourages ethical behaviour or encourages unethical behaviour.*



Corporate culture shapes the values that determine how individuals react to ethical dilemmas.

6. *It evades ethical problems by sending them to the legal or accounting departments.*

Ethics is more than simply complying with laws and regulations. Existing laws and regulations may not cover the ethical dilemma. A lawful act might still be considered unethical.

7. *It looks at ethics solely as a public relations strategy to enhance its image.*

This puts form above substance. It obscures potential ethical problems, and might put the organisation under scrutiny by the media and others.

8. *It treats its employees and clients differently. Where there is no respect for integrity, corruption flourishes.*

Lack of respect for employees creates distrust and hostility that can lead to corrupt activity and make it difficult to resolve ethical dilemmas originating outside the organisation.

9. *It is unfair or arbitrary in its performance-appraisal.*

Inconsistent standards lead to favouritism, cronyism and biased management, which damage morale.

10. *It has no formal procedures or policies for handling ethical problems. Trial-and-error tactics often indicate poor management.*

Guidelines on ethics need to be formulated before problems arise, although discussion groups may be needed to ensure that remedial action does not complicate a particular problem.

11. *It does not provide mechanisms for 'whistleblowing'.*

If complainants are protected, staff will realise that unethical behaviour will not be condoned (see section 5.2).

12. *It lacks clear lines of internal communication.*

Poor communication allows problems to get out of hand before managers realise that they have arisen and can respond to them.

13. *A public sector organisation that is sensitive only to the needs and demands of its ministerial head or a private sector organisation that puts the interests of shareholders above the interests of its customers and employees.*

In the public sector, the minister's interests are central to the functioning of the organisation. However, other individuals and groups have a stake in the actions of the organisation and their views must not be overlooked.

In the private sector, the interests of employees and others are important to support the financial interests of shareholders.

14. *It encourages people to leave their personal ethical values at home.*

When staff are encouraged to ignore their personal ethics at work, a dichotomy exists and impropriety is likely to occur.

Cooke's indicators are only a few of the many danger signs that may be present when an organisation is at ethical risk. You might be tempted to think that these indicators do not apply to your organisation. If so, you should think again.

### **3.11 Adopting an ethical code to prevent corruption**

Proactive prevention involves more than risk assessment and the introduction of timely audits. It also requires a code of conduct to deal with specific situations faced by staff.

Your code should address issues such as private use of agency resources, approval procedures, whistleblowing, acceptance of gifts, conflict of interest, and the principle of random checks.

### **3.12 In conclusion**

Dealing with corruption is a corporate as well as an individual ethical responsibility.

While corruption depends on individuals, it may be unwittingly encouraged or protected by certain features of an organisation's activities or resources.

All public organisations have an obligation to assess the risks of corruption and to ensure that prevention measures are put into place.

In the past, exposing corruption has required a great deal of honesty and courage. An organisation can lift the burden from individuals by adopting effective corruption prevention practices, thereby underscoring its social responsibility and commitment to high ethical standards.

## 4. THE NATURE OF CORRUPTION

### 4.1 What is corruption?

Corruption is criminal behaviour that may involve fraud, theft, the misuse of position or authority or other acts that are unacceptable to an organisation and which may cause loss to the organisation, its clients or general community. It may also include other elements such as breaches of trust and confidentiality.

Corruption is often motivated by greed and flourishes in an atmosphere of management neglect or where there are inadequate controls, checks and balances. It damages an organisation, so, when the cost of corruption is better understood by the community, pressure increases on managers to manage their organisation's performance in ways which will provide better control of corruption.

The Commonwealth's White Paper *Review of Systems for Dealing with Fraud Against the Commonwealth* describes fraud as 'a variety of offences that usually involve deceit, an intention to deceive or deliberate non-disclosure, and some actual or possible injury to the victim of the offence.'

The Queensland *Criminal Code* legislates against the following offences:

- Official corruption (s. 87)
- Extortion by public officials (s. 88)
- Public officers' interest in a contract (s. 89)
- False claims by officials (s. 19)
- Stealing (sections 391 and 398)
- Misappropriation of property (s. 408C)

- Obtaining goods or credit by false pretence or wilful false promise (s. 427)
- Receipt or solicitation of secret commissions by an agent (s. 442B)
- Forgery (s. 488)

Chapter 13 of the Code deals with other offences.

### 4.2 Official misconduct

Corrupt conduct by a public official in Queensland is called *official misconduct* in the *Criminal Justice Act*. It can involve

- carrying out duties in a dishonest way or in a way that lacks impartiality
- breaching the community's trust
- the improper release of confidential information.

Misconduct is defined in sections 2.22 and 2.23 of the *Criminal Justice Act*:

#### Section 2.23 General nature of official misconduct

(1) Official misconduct is -

- (a) conduct of a person, whether or not he holds an appointment in a unit of public administration, that adversely affects, or could adversely affect, direct or indirectly, the honest and impartial discharge of functions or exercise of powers or authority of a unit of public administration or of any person holding an appointment therein;
- (b) conduct of a person while he holds or held an appointment in a unit of public administration -
  - (i) that constitutes or involves the discharge of his functions or exercise of his powers or authority, as the holder of the appointment, in a manner that is not honest or is not impartial;
  - or
  - (ii) that constitutes or involves a breach of the trust placed in him by reason of his holding the appointment in a unit of public administration;

or

- (c) conduct that involves the misuse by any person of information or material that he has acquired in or in connexion with the discharge of his functions or exercise of his powers or authority as the holder of an appointment in a unit of public administration, whether the misuse is for the benefit of himself or another person,

and in any case, constitutes or could constitute -

- (d) in the case of conduct of a person who is the holder of an appointment in the unit of public administration, a criminal offence, or a disciplinary breach that provides reasonable grounds for termination of the person's services in the unit of public administration;
- (e) in the case of any other person, a criminal offence.
- (2) It is irrelevant that proceedings or action in respect of an offence to which the conduct is relevant can no longer be brought or continued in that action for termination of services on account of the conduct can no longer be taken.
- (3) A conspiracy or an attempt to engage in conduct, such as is referred to in subsection (1) is not excluded by that subsection from being official misconduct if, had the conspiracy or attempt been brought to fruition in further conduct, the further conduct could constitute or involve an offence or grounds referred to in subsection (1).

#### **4.3 Management responsibility for corruption prevention**

Managers are required to establish and maintain control systems to ensure that resources are protected. Corruption prevention is integral to planning, management, organising, controlling and leading the organisation.

##### **4.3.1 Prevention**

The prevention of corruption is primarily a management responsibility, but it is a responsibility that must be shared with staff. Internal auditors may suggest prevention and other controls, but management and staff must work together to develop effective strategies.

##### **4.3.2 Detection**

The detection of corrupt activities is a management responsibility, achieved partly by setting up effective control systems, but also by managers being alert to indicators of corruption. With appropriate training, staff can help – if they are motivated to do so through appropriate training and an ethical code.

Internal auditors can also assist the detection of corruption through their advice to management about detection controls, and through their audits. Senior managers may detect incidents, or at least indicators, of corruption through the work of properly focused audits. Security and finance staff have a key responsibility to detect intruders, thieves and embezzlers.

Valuable detection work can be carried out through timely surveillance and random checks of systems.

##### **4.3.3 Notification**

The CJC and the QPS must be notified as soon as there is **reasonable suspicion** of corrupt activity. Investigation is a specialised task which, if mishandled, can easily destroy opportunities to collect evidence. Internal auditors may investigate the circumstances of corruption but are usually untrained in compiling evidence on which to base a conviction. Therefore a notification must be made as soon as there is reasonable suspicion that corrupt activity is taking place.

When public sector organisations in Queensland suspect some form of corruption, their principal officer has a statutory obligation under the *Criminal Justice Act* to notify the CJC, who will decide which is the most appropriate agency to carry out investigation. Most matters are referred back to the reporting agency for internal investigation. More serious matters are referred to the police or investigated by CJC staff.

##### **4.3.4 Prosecution**

Prosecution is the final stage. Where corruption is proven, the Director of Public Prosecutions will decide if and how to proceed.

#### **4.4 Potential corruption sources**

Corrupt activity can involve managers, staff, clients, suppliers, and others who have the motive, access and opportunity to subvert systems for personal gain.

##### **4.4.1 Managers**

Managers are a potentially high risk because their offences can involve serious breaches of trust, because the amounts involved may be large, and because the opportunity for concealment is high.

Managers often know how to bypass the control systems. This allows corruption or fraud in the purchasing process when the authority to order, to approve and to receive goods is loosely supervised and the opportunity exists to "do deals".

##### **4.4.2 Staff**

Staff are at risk when duties are combined to allow access to goods and services and opportunity to use them corruptly. Temptations are especially great in high-risk areas.

##### **4.4.3 Clients**

Clients may be corrupt when they receive funds or grants from a public sector organisation or pay money to an organisation in exchange for goods or services. This can include fee or taxation avoidance, social security scams, over-claimed training and other benefits, under-declared revenues or other fees, and mis-stated registration or licence conditions and entitlements.

##### **4.4.4 Suppliers and contractors**

Suppliers and contractors can be involved in fraud, improper service delivery and construction scams. They may subvert tender processes, short-deliver or over-supply on quantity or quality, or overcharge.

##### **4.4.5 Other parties**

These can include the general public, members of special interest groups and industry representatives.

You should profile key personnel in your organisation in terms of their risk of being corrupted. Figure 1 provides a spreadsheet you can complete based on the model in Figure 1M.

For further information on corruption risks, see section 5.5.

FIGURE 1M

MODEL ASSESSMENT OF PERSONNEL AT RISK

RISK SOURCE	THEFT	WRONG SUPPLY	MALICIOUS DAMAGE	BRIBERY	UNDUE INFLUENCE	NEGLECT OF DUTY	UNAUTHORISED ACTIONS	MISUSE RESOURCES	INVALID INFORMATION	FORGERY	SUMMARY RISK
Management				X	X		X	X			
Staff	X			X		X		X		X	
Clients				X	X				X		
Suppliers		X		X							
Others											
<b>SUMMARY RISK</b>											

- Place a cross in the appropriate box.

**FIGURE 1** **ASSESSMENT OF PERSONNEL AT RISK**

RISK SOURCE	THEFT	WRONG SUPPLY	MALICIOUS DAMAGE	BRIBERY	UNDUE INFLUENCE	NEGLECT OF DUTY	UNAUTHORISED ACTIONS	MISUSE RESOURCES	INVALID INFORMATION	FORGERY	SUMMARY RISK
Management											
Staff											
Clients											
Suppliers											
Others											
<b>SUMMARY RISK</b>											

- Place a cross in the appropriate box.

#### 4.5 Corruption categories

*Organised corruption* involves several participants in a structure and hierarchy, acting in a premeditated way.

*Vogue corruption* involves many participants using a "rip-off" scheme that has become popular.

*Repetitive corruption* involves a single participant conducting numerous offences of a similar nature over a period of time.

*One-off corruption* involves one person in a single offence or a series of single different offences.

#### 4.6 Allegations received by the CJC

Many allegations of official misconduct have been made to the CJC over the last three years. The categories we set up to handle these complaints may help you assess the potential for corruption in your organisation. They are:

- assault
- corrupt behaviour
- favouritism
- false evidence
- theft of goods/property
- harassment of staff or clients
- information breeches
- failure to do duty
- misuse of powers
- criminal acts and omissions.

#### 4.7 Typical corruption symptoms (red flags)

As mentioned earlier, red flags can be used to detect corrupt behaviour. While the presence of red flags is not conclusive evidence of corrupt activity, generally, the more red flags you notice, the greater the risk of corruption.

Complete the checklist that follows for red flags that apply to your organisation. This will identify specific areas that you will need to address in your design of corruption controls.

#### 4.7.1 Staff

- ☐ Excessive pressure to perform.
- ☐ Incentives for super performance.
- ☐ Performance that is too good (or bad) to be believed.
- ☐ Illogical excuses and reasons for unusual events or actions.
- ☐ Bad temper, frequent absenteeism, excessive phone calls.
- ☐ Idle time, late starts, early finishes, gross untidiness.
- ☐ Open access allowing some people special access to resources at certain times, particularly to the inventory.
- ☐ Supplier's address that is the same as an employee's.
- ☐ Unusual familiarity between staff and clients or suppliers.
- ☐ Staff who work excessive hours or who do not take holidays.
- ☐ Senior staff involved in "junior" work, such as purchasing, ordering and receiving.
- ☐ Excessive levels of staff turnover.
- ☐ Open disrespect for senior managers.
- ☐ Potential conflicts of interest not covered by required declarations by staff.
- ☐ Excessive number of duties residing with one person.
- ☐ Undue secrecy, or excluding people from normally available information.
- ☐ Excessive spending habits on taxis, lunches, holidays, recreational activities, clothing, entertainment and gambling.
- ☐ People with high debts or assets, unsustainable or unrelated to their income.
- ☐ People who treat controls and standard practice as challenges to be overcome or defied.

**4.7.2 Transactions**

- ☐ Transaction splitting that puts certain transactions below a level that would require review. This can occur with tenders, purchase orders and expense vouchers.
- ☐ Inventory shortages and adjustments.
- ☐ Excessive credit notes, refunds or client-account adjustments.
- ☐ Different suppliers with the same address.
- ☐ Shortages on delivery from a supplier.
- ☐ Deviation from specifications agreed to by a supplier without adequate notification or explanation.
- ☐ The lowest-price quotation not accepted.
- ☐ Requests for delayed inspection of goods or services from clients or applicants.
- ☐ Cheques or statements given to staff for handing to suppliers or clients.
- ☐ Customer complaints that payments are not processed or that statement balances do not represent their transactions.
- ☐ Excessive levels of waived late payment charges.
- ☐ Terminated employees still appearing on the payroll.
- ☐ Large cash transactions, in which cheque payment or account transactions would normally be expected.
- ☐ Internal audits assigned to non-audit tasks.

**4.7.3 Documentation**

- ☐ Missing documentation required to complete an application or request.
- ☐ Missing information on an application or request form.

- ☐ "Blind" approval, where the signatory does not see or review the supporting documentation.
- ☐ Coerced approval, as in, "just sign this for me quickly, I'm in a hurry".
- ☐ Approval by the preparer.
- ☐ Single approval.
- ☐ Adjustments not approved by the appropriate person.
- ☐ Hand-written supplier invoices.
- ☐ Invoices that are duplicates or copies with the original not reasonably accounted for.
- ☐ Supplier accounts opened and supported by hand-written documents supplied by staff in remote locations.
- ☐ Cheque signatories who approve payment.
- ☐ Overs or unders in cash takings, compared with the cash-register or other records.
- ☐ No separate invoice number series for cash sales.
- ☐ A separate cash register for receipts not included in the takings.
- ☐ Excessive voids or refunds on a cash register.
- ☐ Deposits in transit that are "slow" reaching the bank.
- ☐ Unpresented cheques that are slow to be cleared from the bank reconciliation, particularly when they refer to unusual transactions or occasional payees.
- ☐ In-transit entries growing rather than clearing.
- ☐ Data input totals that disagree with computer reports.
- ☐ Alterations of documents such as day books, logs and time records.



#### 4.7.4 Audit

- ☐ Superior performance by a new staff person compared to work record of the previous employee.
- ☐ Any attempt to limit the information available to the auditors, internal or external.
- ☐ Failure to bring recording and processing up to date during periods of rapid growth.
- ☐ Lack of respect for accounting and information reports.

#### 4.8 A selection of incidents

The possibilities for corruption are limited only by the imagination of those who seek to subvert the system for their own personal gain. The following incidents or allegations of corrupt behaviour are representative extracts drawn from our files. They may alert you to vulnerable areas in your organisation that require better prevention and detection strategies.

- **Railways employees** were alleged to have stolen beer and other goods transported by rail.
- **Minister of the Crown** intervened to cause a favourable rezoning for a resort owner.
- **Complainant** was subjected to sexual advances by an investigator from a public service department.
- **Store-owner** alleged that a public service employee maliciously prosecuted him for possessing meat not butchered according to health regulations.
- **Driving examiner** was alleged to have sexually harassed clients and offered to pass female applicants in exchange for sexual favours.
- **Lecturer** alleged corrupt selection practices in the choice of senior staff at a tertiary institution.
- **Salaries clerk** received money to which he was not entitled by corrupting a computer program.
- **Councillor** failed to clear his interest in a parcel of land under consideration for rezoning.
- **Medical practitioner** employed as a visiting specialist at a public hospital charged for services which he did not perform.
- **Mining warden** was alleged to have cancelled a mining lease without issuing the proper notifications. He then registered that lease in favour of a family member.
- **Clerk of a court** misappropriated funds from the office's petty cash.
- **Contractor** complained that he was granted council work only after he agreed to carry out work free of charge for a council member.
- **Psychiatric nurse** was disciplined for assaulting a patient in his care.
- **Manager of a statutory authority** was alleged to have improperly obtained a vehicle previously the property of that authority.
- **Public servant** was alleged to have used taxi vouchers for private purposes.
- **Shire building inspector** was alleged to have approved a substandard dwelling as a favour for an associate. The residents of that dwelling then claimed that it should never have been a certificated for occupancy.
- **Employee of educational institution** stole building materials.
- **Race club executive** was alleged to have received benefits in exchange for providing free race-book advertising to an associate.
- **Public servant** on a training course absent from his place of duty was alleged to have claimed more than his travel allowance entitlement.

- **Public sector employees** allegedly used work resources to compile job applications.
- **Bus company proprietor** claimed that a government department improperly authorised the operation of a competitor.
- **Child-care centre worker** was alleged to have misapplied government grant monies intended for the specific use of another centre.
- **School principal** was alleged to have deliberately overstated the number of students on the roll of his school to attract increased departmental funding.
- **Council worker** was alleged to have successfully purchased an ex-council vehicle for sale by tender because of his knowledge of the other bids.
- **Shire chairman** required mechanics in the council workshop to carry out repairs on his personal vehicle.
- **Ratepayer** said his property had been subject to flooding caused by filling in a neighbouring property; the action had been approved by the council though it was evident that problems would follow.
- **Council employees** stole "scrap" materials from a council workshop.
- **Councillor** claimed that she was victimised by council employees who refused to provide information to which she was entitled.
- **Public service counsellor** was alleged to have been over-familiar with clients.
- **Property owner** believed that his faulty dwelling was approved by council because of a relationship between the builder and the council building inspector.
- **Ratepayer** complained that a rezoning application was unsuccessful despite identical rezoning by a neighbour who was a council member.
- **Ratepayer** suspected council impropriety because the council apparently refused to take action against

a neighbour who openly advertised and conducted an engineering business in an area zoned residential.

- **Motorist** reported receiving an infringement notice pertaining to a vehicle he had de-registered some months before. An official had not destroyed the forfeited registration plates, but had given them to a third party.
- **Council** imposed new parking regulations without making the concomitant by-law amendments.

#### 4.9 Corruption in local government authorities

In July 1991 we reported on six investigations of alleged corrupt conduct or official misconduct in local government authorities. The details below demonstrate how corruption may be sustained in any organisation with inadequate controls.

##### 4.9.1 Case A

A vehicle-maintenance service company had been a preferred supplier to a local council for more than twelve years. No real effort had been made to investigate any other supplier, and the council's purchasing officer had a close social relationship with the supplier.

Overpricing and invoice errors in favour of the supplier were common and the council had no adequate procedures by which to verify the charges.

Purchase orders were not issued nor were the vehicles inspected by the council's workshop supervisor before maintenance was provided. Confirmation orders were always prepared after the work was completed.

The administrative system had clearly broken down to the extent that there was tacit acceptance of the arrangement with the supplier among a wide section of council staff.

The internal audit program did not pay sufficient attention to abnormal patterns of purchasing, ordering and authorisation.

##### 4.9.2 Case B

A Shire council chairman, who had held his position for nearly twenty years, was also the principal contractor in a grass-slashing operation. He declared this interest in 1984. He did not

reveal his interest in the companies of two other contractors, for whom he submitted invoices.

The appointment of private contractors was not adequately recorded or controlled by the shire. The chairman used his influence to appoint a particular contractor.

No record of completed work was kept by the council, nor was any record submitted by the contractors to support their invoices.

The chairperson signed cheques payable to himself and to the other contractors. Such an action may not have been contrary to Local Government Audit Regulations, but it indicated poor internal control.

Cheques payable to one contractor were endorsed and paid into the chairman's bank account. There was no procedure to examine endorsements.

#### **4.9.3 Case C**

A contract for servicing refuse tips was called and four companies responded. After one tender was accepted (not the lowest), the contract terms were substantially changed. The annual cost increased from \$60,000 to \$160,000.

The town clerk negotiated the changes to the contract without informing the engineer or health surveyor. The contract was not re-tendered to allow all four contractors to be considered.

A contract worth more than \$50,000 was let without calling for quotations as required by the *Local Government Act*. One supplier submitted four separate quotations for the contract.

An alderman was involved actively in the consideration and negotiation of these contracts.

#### **4.9.4 Case D**

A councillor declared a pecuniary interest but nevertheless participated in deliberation of issues related to the matter. This action contravened the Oath of Office under the *Local Government Act*.

The councillor claimed the cost of private work done by him on a boat ramp, when council had not approved the work. The councillor's claim was paid when the costs were included with other work done by the councillor in his private capacity. The cost was not reimbursed by the councillor, but by other parties.

#### **4.9.5 Case E**

Private expenses were charged to the council by the town clerk and other senior council officers. The chairman of the finance committee, who was the ultimate approval authority for such expenditure, was present at most functions. The council had given no clear guidelines for the use of credit cards.

Information on vouchers failed to describe the expenditure adequately, although it was approved by the finance committee. The expenditure was for entertainment, air fares, accommodation and gifts.

#### **4.9.6 Case F**

A council foreman allocated work to truck and equipment owner-drivers. The foreman had a personal interest in some of the hired plant, but had not declared a pecuniary interest as required by council policy. Senior council officers were actively involved in the matter and condoned non-disclosure.

There was no adequate system to control the unbiased allocation of work to owner-drivers.

### **4.10 Discussion of local government case studies**

We identified the following problems:

- inadequate financial control and records, and poor financial and operational systems and procedures
- audit procedures that checked only financial documentation and accounts
- lack of checks and balances within the system to ensure that areas or rights and transactions could be identified
- administrative arrangements that resulted in senior officers associating closely with the council of the day and being dependent upon influential members of the council for their employment and advancement
- little awareness among employees and council members of matters involving possible conflicts of interest, compounded by an unwillingness of administrators and the Department of Housing and Local Government to enforce the relevant legislative provisions.

## 5. PREPARING FOR CORRUPTION PREVENTION

### 5.1 Corruption control concerns everyone

Managers may overlook red flags because they cannot be everywhere at once, but staff can contribute to corruption prevention when the corporate ethos encourages them to be alert and to report suspicious activity. Staff are more likely to detect corrupt behaviour if they are trained to recognise and respond to red flags or other telltale signs. However it is one thing to be aware of corrupt activity and another to report it.

### 5.2 Whistleblowers

Although crime affects us all, the first instinct of many who are faced with what seems to be corrupt behaviour is not to get involved. They might not approve of what is happening, but, for many reasons, they take no action, especially against friends or colleagues. This creates a climate of secrecy so that, when the "good guys" refuse to help fight corruption, the "bad guys" win.

In 1988 the South Australian State Government Insurance Commission surveyed community attitudes towards third-party insurance fraud. It found that "dobbing" was widely held to be unacceptable. However if the "dobbing" involved a crime involving drugs or violence, it was seen in a different light from attempts to "rip off the system".

When researchers pointed out that it was not the Government who lost these resources but the taxpayers, there was a perceptible shift in attitude. Respondents then said: 'If there was a campaign to dob in frauds, I'd dob them in'.

Some people recognise that corruption in the public sector hurts the entire community, and this leads them to become whistleblowers.

Whistleblowers pose a dilemma for some managers. You might find it revealing to test the attitude of managers in your organisation towards those who have reported suspicious behaviour. Consider how you and they would react if a member of staff reported corruption in your area of control. Would you feel as though the informant had betrayed a trust?

The evidence in many Australian states suggests that people who would never contemplate defrauding the system actively resent, and have frequently persecuted, informants. This will stop only when we accept that everyone has a duty to report corruption. If honest people can be intimidated, the criminals win.

The challenge here is not simply how to make your control strategies more effective and efficient, but also how to encourage staff to support whistleblowers.

### 5.3 Individual rights in investigations

Individual rights need to be safeguarded. Before developing your prevention plan, think about the following, which may influence how your strategy is formulated and marketed:

- Corruption investigators are sometimes accused of denying the fundamental individual rights of those being investigated. Should those rights be regarded as absolute, or should they be seen as part of a body of competing interests?
- Should those interests not only include protection from the consequences of intrusive investigations, but also take into account protection from the consequences of the corrupt conduct of others?
- Is the balancing of those competing interests up to the Government or the investigating agency?

In an address to the fourth International Anti-Corruption Conference in Sydney in 1989, Mr A Roden QC, Assistant Commissioner of the NSW Independent Commission Against Corruption, described the delicate balance that must be struck between conflicting community and individual interests.

The interests of the individual are supreme. Yet I am about to argue that, on the basis of that proposition, in the area of corruption control there is justification for limiting, or even denying, what many civil libertarian colleagues regard as inalienable individual rights.

I approach the balancing process with two principles in mind:

- it is the right of every individual that due regard be had to his or her interests; but
- there is no warrant for asserting that any particular interest of any particular individual shall prevail over all others.

The individual rights that have to be considered are:

- the right to privacy
- the right to silence and the privilege against self-incrimination
- fundamental principles of natural justice including the right to know the nature of any allegation made, the right to confront and challenge one's accuser, and the right to answer allegations at an early stage of the investigation
- freedom from public disclosure of unproven allegations
- respect for the integrity of person and property
- the right to fair and impartial treatment at the hands of public authorities and public officials.

Roden argues that these rights cannot always co-exist and that they are, in his view, not absolute rights but competing interests.

He indicates that the following factors qualify corruption investigations for special powers:

- By its very nature official corruption is likely to occur in secret transactions and involve people who are in a position to participate in its concealment. Accordingly more powerful and more intrusive means of investigation than those commonly available are likely to be needed.
- Official corruption can occur in the highest places and the higher it strikes, the greater the danger it poses.

- Corruption among holders of public office has the capacity to undermine the very institutions which protect the individual rights and interests we are concerned to preserve. Accordingly, exceptional weight must be given to maintenance of the integrity of public institutions.

- The principal goal is the maintenance of the integrity of public institutions and the exposure and minimisation of the corruption is more important than simply securing the conviction of individual offenders.

## 5.4 Corruption prevention models

In the past, many organisations have taken two approaches to counter corruption.

The first is an *accountancy-based* model where the skills of auditors and accountants are employed to examine financial systems to make it more difficult for people to embezzle or defraud.

The second is a *policing* model that investigates allegations of corruption and prosecutes those found to be corrupt.

While these approaches are an important part of a prevention strategy, behaviour modification and enlightened staff management are also essential. In a *management-based* model, managers are required to be aware of those elements that are at risk and to take proactive steps to discourage staff from becoming involved in corrupt activity. To better understand this model we must first consider the reasons why people become corrupt.

### 5.4.1 Who might be tempted to be corrupt?

In *Fraud Auditing and Forensic Accounting* Jack Bologna and Robert Lindquist suggest that

- some people are honest all of the time
- some people (fewer than the above) are dishonest all the time
- most people are honest some of the time
- some people are honest most of the time.

The effective manager will presume that most staff strive to be honest but will be aware that some staff may not have an honest approach.

In *Lying, Cheating and Stealing* Gwynn Nettler offers these insights on cheaters and deceivers:

- people who have experienced failure are more likely to cheat
- people who are disliked and who dislike themselves tend to be more deceitful
- people who are impulsive, distractable, and unable to postpone gratification are more likely to engage in deceitful crimes
- people who have a conscience (fear apprehension, and punishment) are more resistant to the temptation to deceive
- the easier it is to cheat and steal, the more likely it is that people will do so
- individuals have different needs and therefore they have different levels at which they will be moved to lie, cheat, or steal
- lying, cheating, and stealing increase when people are placed under unreasonable pressure to achieve objectives
- the struggle to survive may generate deceit.
- they may think: *They're so big, stealing a little bit won't hurt them*
- they do not know how to manage their finances, and so they might believe that they are forced to steal to pay debts
- they feel that outwitting the organisation is a challenge and not a matter of economic gain
- they have been economically, socially, or culturally deprived during childhood and are compensating for a void felt in their personal life so they lie, cheat or steal as a compensation for lack of love, affection, and friendship
- they lack self-control and they steal out of compulsion
- they believe that either they or friends at work have been subjected to a humiliation or abuse, or have been treated unfairly, and they seek ways to pay the organisation back for the perceived injustice
- they tend to be unwilling to work for those things they want or need
- they face constant temptation to steal because the organisation's internal controls are lax
- they believe that no one has ever been prosecuted for stealing from the organisation

#### 5.4.2 Why people lie, cheat and steal at work

Nettler also lists attitudes that may motivate people to lie, cheat and steal at work:

- they believe that they can get away with it
- they may think they desperately need or desire the money or articles stolen
- they feel frustrated or dissatisfied about some aspect of their job
- they feel frustrated or dissatisfied about some aspect of their personal life that is not job-related
- they feel abused by the employer and want to get even
- they fail to consider the consequences of being caught
- they may think: *Everyone else steals, so why not me?*
- many thieving employee are caught by accident rather than by audit or by design; therefore, fear of being caught may not be an effective deterrent to theft
- employees are neither encouraged to discuss personal or financial problems at work nor to seek management's advice and counsel on such matters
- theft by employees is not a work-related issue; each theft has its own conditions, and each thief has his or her own motives
- once motivated, employees may steal for as many reasons as their imagination can conjure up
- they believe that employees never go to jail or receive harsh prison sentences for fraud, stealing, or embezzling from their organisation.

### 5.4.3 Characteristics of corrupt people

Corrupt people are more likely to display certain characteristics. They may

- live beyond their means
- have a very great desire for personal gain
- have a high level of personal debt
- enjoy very close relationships with clients or suppliers
- believe that their salary is not commensurate with their responsibilities
- have a "wheeler-dealer" attitude; that is believe that rules are for others
- treat corruption controls in the system as a "challenge"
- have an excessive gambling habit
- suffer significant family or peer pressure.

While these are general characteristics, people who exhibit one or more of them may need to be monitored or possibly reviewed, especially if they can act autonomously and have the authority or opportunity to override or subvert control procedures that normally apply.

### 5.5 Management accountability

Management accountability is perhaps the most difficult element to incorporate into a prevention program. At its simplest, accountability means that managers cannot not plead ignorance when corruption is discovered in their areas. Such ignorance could be a *prima facie* case for poor supervision.

Accountability should be established by senior managers who must describe it in positive as well as negative terms. Unfortunately, accountability often only comes into play when blame is being assigned. Too often junior staff get the blame because senior staff are better at avoiding it. Senior managers must guard against accountability becoming merely an exercise in self-justification.

In a complex management environment it is unrealistic to expect that every transaction or decision can be assessed for criminal intent. Managers must identify the most vulnerable elements of their programs and concentrate their resources in those areas.

This is not easy. It exposes the organisation to corruption in areas assessed as low risk. Managers should seek advice from staff throughout the organisation and apply the best available risk management techniques.

### 5.6 Corruption prevention is better than cure

Prevention is better than dealing with corruption after it has occurred because it is less damaging to the organisation.

Corruption detection and investigation is a disrupting, extensive and costly process. Managers should consider the long-term benefits of active prevention through improved risk assessment, personnel management and staff training.

Simple prevention systems are often easy to establish and maintain. Sometimes only simple systems are necessary to deter people from corrupt activity. When there is a deliberate and systematic attempt to subvert the system, however, specialised controls will be required.

### 5.7 High risks areas are easier to predict

Where it can be predicted, corruption can be prevented and deterred by the use of effective control systems. It may help if we look more closely at the generic types of corruption.

#### 5.7.1 Theft

Theft can involve stealing, pilfering and other unauthorised taking of goods or materials. Theft may include unauthorised borrowing of goods or materials, or the use of employee time other than for the employer's business.

Minor theft is sometimes tolerated. For example, personal phone calls may be tolerated if they do not significantly reduce the efficiency of the organisation.

### 5.7.2 Wrong supply

Wrong supply applies mainly to purchasing. Supply may be deliberately short-delivered and the cost maintained, or supply may be over-delivered and the cost increased.

Wrong supply can apply when consulting, maintenance or construction services are deceitfully provided without an opportunity for the client to verify the quantity or quality.

### 5.7.3 Malicious damage

The physical assets of an organisation may be damaged by disgruntled staff or outsiders. Staff may attack computer files for revenge against the organisation or a specific manager. Computer hackers may cause damage for other reasons.

### 5.7.4 Bribery

A supplier or client may offer a bribe to staff in return for favoured treatment. The giver and the receiver are equally culpable.

Bribes may be gifts. These can include lunches, presents, tickets to sporting events, free travel and heavy personal discounts. There may be no guidelines about the type and value of gifts that suppliers or clients can give to staff.

Other organisations have defined acceptable levels and determined who may accept gifts and in what circumstances. Often, such gifts only need to be declared by the receiver. Procedures for receiving gifts should be clearly defined in your code of conduct and made known to all staff.

You should be aware that s. 625(4) of the *Queensland Public Finance Standards* refers to 'reportable gifts'. These standards apply to all public sector units.

### 5.7.5 Undue influence and power

This can involve misuse of authority by an official or member of staff but it may also be used by a supplier or client against a staff member. Undue influence can also be used to disadvantage one party in favour of another.

Power of this kind may be subtle. It can be an act based upon deception. While it provides potential benefit to the power player, it can damage an organisation's resources or reputation.

Many organisations have advisory committees and boards which may include representatives with a vested interest. These people are supposed to declare such conflicts but may not always do so.

### 5.7.6 Neglect of duty

Neglect of duty can result from bribery or undue influence. Neglect may include the failure to

- inform a client of particular conditions or requirements
- inform senior staff of discussions with, or requirements that were not satisfied by, the supplier or client
- ask for information from a client or supplier, knowing that this information could disqualify the client or supplier from some entitlement
- inspect premises, objects or information to avoid an unfavourable assessment
- assess circumstances according to the required criteria, when this would produce a result less favourable to a supplier or client
- take action even though facts and circumstances indicate it is required.

Neglect of duty may also include deception. It could involve more than mere negligence or failure to act with due diligence.

### 5.7.7 Unauthorised actions

Staff can exceed their authority to purchase materials, or provide information or grant entitlements. Clients may exceed the authority granted to them by a licence or registration.

Unauthorised actions can include using authorised access to goods, services or information for unauthorised purposes. A manager might entertain friends or family on a business expense account. A purchasing officer may include in an order some goods delivered to a personal address. A manager might hire out equipment to gain income.



#### 5.7.8 Misuse of resources

This involves using an organisation's facilities for personal use. For example, personal records may be kept on the organisation's computer systems. "Foreign orders", that is, private orders, might be made up in the organisation's workshops.

#### 5.7.9 Invalid information

Invalid information includes

- data supplied by clients that serve as the basis of payments by them (levies) or to them (grants)
- data wrongly classified to reduce a levy or increase a grant, when the amount varies between classifications, or data overstated or understated, to achieve the same result
- incomplete data, supplied by clients, that allow them to obtain benefits to which they are not entitled.

#### 5.7.10 Forgery

Forgery can make false documents appear genuine. Signatures can be forged on cheques or purchase orders, and altered and photocopied invoices can be used to get unauthorised payments.

Forgeries can support applications for entitlements for which the applicant is not eligible. For example, an applicant may make double or multiple claims for one benefit using forged documents.

Fictitious information may be provided to support an application for a pension or entitlement card. A stolen credit card may be used to verify a false application.

#### 5.8 Developing a corruption prevention policy

The first step is to appoint a *corruption management committee* to develop an appropriate policy, which is then communicated to your staff. The policy should include

- directions to managers that they are responsible and accountable for establishing and maintaining control

procedures to prevent and detect corruption

- communication to staff that corruption is unacceptable and that offenders will be disciplined and/or prosecuted
- communication to staff that the internal auditors have a responsibility to assess the corruption risks to evaluate prevention procedures, and to be alert to and audit for possible incidents of corruption
- means by which staff undertake to reject corrupt behaviour, become aware of the potential for corruption and recognise its symptoms
- a procedure for staff to report suspected corruption to an official in the organisation or directly to the CJC without fear of recrimination
- a plan to ensure that no staff reporting corrupt behaviour will be disadvantaged for reporting their suspicions.

#### 5.9 The corruption prevention plan

The corruption prevention plan should be supported by the corporate plan and other management plans. It should relate to all of the organisation's programs and resources and reflect the organisation's basic corruption prevention policy.

##### 5.9.1 Relationship to other plans

*The corporate plan* defines the organisation's mission, objectives and program goals; it also specifies key performance indicators. The corporate plan should include a comment by the chief executive on the importance of corruption prevention.

*The business plan*, reflected by the annual budget, should describe the resources that will be applied to corruption prevention. Program budget goals require managers to be alert to the risk of loss through corruption. The need for project corruption control – to ensure that the business receives value-for-money and to eliminate corruption – should be mentioned in the discussion supporting the financial summaries in the budget documents.

The *internal audit plan* should give priority to corruption prevention by covering it at three levels:

- in the internal audit charter, as a basic responsibility
- in specific projects, to support the corruption prevention activities of managers and other staff
- in all projects, to eliminate the risks identified by control evaluation.

### 5.9.2 Contents of a corruption prevention plan

The following are possible components of the corruption prevention plan:

- covering letter
- title page
- table of contents
- executive summary
- corruption prevention strategies and policies issued by senior management
- results of the risk analysis
- recommended control improvements
- responsibilities, priorities, deadlines.

### 5.10 A corruption prevention strategy

Once the policy and plan have been articulated, a strategy must be developed which

- identifies the people responsible for corruption prevention in the organisation
- maps out the steps to take to prevent, detect and report corrupt activities.

You should form a *corruption risk assessment committee* to undertake a risk analysis and develop and implement a plan to

- develop staff awareness of the red flags that indicate potential corruption
- develop management and staff support for controls and timely checks and balances
- develop an incident information system

that monitors exposure to corruption and advises managers and staff of relevant incidents

- document prevention procedures and train staff
- coordinate internal and external prevention resources.

### 5.11 Corruption prevention officers

Corruption prevention duties should be included in key staff duty statements. Corruption prevention officers may include managers, members of risk assessment committees, internal auditors, security officers, inspectors, personnel managers, staff in the legal section and purchasing supervisors. They should meet as a *corruption prevention committee* to discuss common concerns. Plans, techniques, corruption experiences, training initiatives or activities can be shared.

A total resource action plan should be developed and reviewed regularly. Consultants and other external personnel such as security service providers and advisers, and risk management experts activities need to be co-ordinated by the internal prevention staff to avoid overlap, to minimise cost and to increase effectiveness.

### 5.12 The corruption prevention staff register

The next step is for the management committee to develop a staff register, which could list the

- corruption prevention officer(s)
- number of people and budget under his or her control
- responsibilities of the officer
- key relationships of the officer in the organisation
- scope of operations under his or her control
- level of specific training received or given
- special skills, resources or contacts
- reporting lines and chains of authority
- a history of corruption prevention activities.

The details will vary according to the particular needs of your organisation.

## 6. ANALYSING THE FINANCIAL CORRUPTION RISKS

This section of the manual focuses on the financial aspects of corruption control. It examines the control of fraud, theft, embezzlement and other risks to the financial integrity of the organisation.

Determining your organisation's level of risk in revenue (income), expenditure, assets and liabilities is an important step in analysing its exposure to corruption. The accounting system and financial registers can be used to identify risks at particular locations or in specific programs. The types of income, expenditure and so on, should be analysed.

A spreadsheet makes it easy to match organisational resources, responsibilities and structure. It can be adapted according to what is being analysed or what is being presented. Tabulations can be reorganised, regrouped and aggregated to analyse financial data into a framework that identifies the areas being assessed. Once the spreadsheet format is established it should remain consistent. For example, programs and locations should be placed in rows, and asset and risk types in columns. Figure 2 provides a basic format. Adapt and photocopy it as necessary for the various sections of your organisation.

### 6.1 Revenue risks

Those who develop the spreadsheet must have detailed knowledge of the program or location at risk because that is where preventive measures and possibly a detection audit will be needed.

This analysis can go through several stages.

Referring to the model (Figure 2M) create a spreadsheet (Figure 2) with types of revenue specific to your organisation in the column headings. List each program or location in the left column. Look at each column heading and decide whether that revenue type exists for that program or location. Use a code such as an 'X' to show a matching cell. Use this method for all areas.

You could also group the revenue into types of risk such as data dependence, price understatement, cash sales register manipulation, and so on.

The type of revenue or income should identify receipts which depend on data provided by the client, such as levies based on production or sales. You may have to refer to other aspects of high risk to decide if corruption is likely.

Work through all forms of revenue, classifying receipts by their exposure or sensitivity to corruption. Different forms of revenue may be subject to the same types of corruption. For example, stocks of surplus equipment and waste products might be sold at give-away prices and might be exposed to the same form of corruption by under-pricing. The waste product could also be under-measured.

**FIGURE 2M      MODEL FINANCIAL DIMENSIONS OF REVENUE**  
**(\$million)**

NO. PROGRAM OR LOCATION	GOVT. APPROP.	SPECIAL FUNDS	PROGRAM LEVIES	LICENCE	INDUSTRY SUBS.	SALES/ SERVICE	TOTAL REVENUE
Brisbane - Chermside	15		1	5			21
Brisbane - Indooroopilly	10	2			1		13
Dalby	15	1		1	1		18
	40	3	1	6	2		52

- Place a dollar amount in the appropriate box.

**THE FINANCIAL DIMENSIONS OF REVENUE**  
(\$million)

[illegible]

- Place a dollar amount in the appropriate box.

## 6.2 Expenditure risks

After examining the model (Figure 3M) prepare a spreadsheet (Figure 3) with program activities and locations in rows and the types of expenditure in columns. Identify the types of expenditure and exposure risks. Again, suit the spreadsheet to your organisation.

- Under salaries, there could be high levels of casual staff with after-hours attendance and difficulty in monitoring them.
- Highly variable overtime with limited supervision could suggest over-stated claims.
- Excess amounts of higher duties or other allowances could indicate unauthorised claims.
- Payments of benefits or grants, which might rely on information provided by beneficiaries, have the potential for over-claiming. These benefits may cover a range of different programs, such as drought or flood relief, research funding, education, health and social benefits.

- Payments for services should ensure that the quantity and quality of services were provided as invoiced. Details of time, attendance and materials to support the payment might not be reliably recorded. This type of expenditure occurs often and is difficult to verify.

- Purchasing, as the stage before expenditure, is exposed to corruption because quantity, quality, price and service can be negotiated on one basis and provided on another.

- Tenders or quotations can be unfairly compared to favour a supplier who would not otherwise have won the contract. Summarising contracts under the headings of annual value, type of goods or services, time since appointment, price increase per cent since contract commencement date, and other corruption data, helps to indicate potential risks.

Separating the expenses in the spreadsheet will identify how much of your organisation's expenditure is at risk.

**FIGURE 3M    MODEL FINANCIAL DIMENSIONS OF EXPENDITURE  
(\$million)**

NO. PROGRAM OR LOCATION	LOCAL GOVT. ALLOCATION	SPECIAL FUNDS	BENEFIT PAID	GRANTS incl R&D	PROGRAM SUPPLY	SALARY	ADMIN SUPPLY	TOTAL EXPENDITURE
Brisbane - Chermside	2	5		3	3	5	3	21
Brisbane - Indooroopilly		3	1	3		3	3	13
Dalby	5	5		2		4	2	18
	7	13	1	8	3	12	8	52

- Place a dollar amount in the appropriate box.

[illegible]

- 30



## **6.3 Resources risks**

Referring to the model (Figure 4M) prepare a spreadsheet (Figure 4) to describe the programs, services or locations of your organisation, and assess the risk of corruption as high, medium or low in terms of assets, finance, staff, external relationships and information.

As shown below, different programs can be exposed to different forms of corruption. More detailed spreadsheets can be developed to describe each type of program.

Information can be exposed to corruption through unauthorised release or from damage caused by the techniques used to store, record and retrieve data. All resources – physical, financial, human and informational – are at risk. Even the organisation's external relationships are corruptible.

Figure 5 provides some prompts to identify information resources at risk.

### **6.3.1 Assets**

Fixed assets can be stolen, misused or subjected to malicious damage. Purchasing of assets can also be a high-risk area.

### **6.3.2 Financial resources**

These include cash of all kinds, funds in bank accounts, investments and treasury operations and funds due to the organisation.

Funds are the most sensitive of assets and the most exposed to corruption.

[The next two categories are not strictly financial resources, but corruption in these areas can have substantial financial implications for the organisation.]

### **6.3.3 Human resources**

Employees can be tempted to neglect their duty, use undue influence, misuse their authority or be the targets for bribery.

There can be a gradual progression from inefficiency to deliberate misuse of time and unauthorised actions for personal gain.

Staff members responsible for the recording as well as the custody of resources are particularly at risk of corruption.

### **6.3.4 Information resources**

Corrupt persons can receive substantial money for providing information held by public sector organisations. Release of other information regarded as sensitive or "commercial in confidence", including information on people's health or financial status that has been obtained in trust from clients or suppliers, also constitutes corrupt behaviour. An organisation may be damaged by the adverse publicity that follows such breaches.

Vast amounts of information resources are kept on computers, both on mainframe and personal computers. Release of this information, or modification of key data fields, are forms of corruption. The deliberate introduction of viruses is an advanced form of corruption.

**FIGURE 4M FINANCIAL DIMENSIONS AND DESCRIPTIONS OF RESOURCES**

[illegible]

- Place a dollar amount under assets and financial resources. Staff can be rotated as a dollar amount or numbers.
- Provide a description for external relationships and information.

**FIGURE 4                      FINANCIAL DIMENSIONS AND DESCRIPTIONS  
   OF RESOURCES**

NO. PROGRAM OR LOCATION	ASSETS	FINANCE RESOURCES	STAFF	EXTERNAL RELATIONSHIPS	INFORMATION

- Place a dollar amount under assets and financial resources. Staff can be rotated as a dollar amount or numbers.
- Provide a description for external relationships and information.

Referring to Figure 5M, summarise the information kept in each program or location in Figure 5 and assess its level of confidentiality in the columns. Where a cell is active, enter an alpha or numeric code and detail the risk in a supporting table.

**FIGURE 5M ANALYSIS OF RISKS TO TYPES OF INFORMATION**

NO. PROGRAM OR LOCATION	PROGRAM SENSITIVE	PROGRAM CONFIDENTIAL	CLIENT CONFIDENTIAL	STAFF CONFIDENTIAL	EDP FILES	EDP DATA	EDP PROGRAMS
Brisbane - Chermside		X	X	X	X	X	X
Brisbane - Indooroopilly	X	X		X	X	X	X
Dalby		X		X	X	X	X

- Place a cross in the appropriate box.

**FIGURE 5**

**ANALYSIS OF RISKS TO TYPES  
OF INFORMATION**

NO. PROGRAM OR LOCATION	PROGRAM SENSITIVE	PROGRAM CONFIDENTIAL	CLIENT CONFIDENTIAL	STAFF CONFIDENTIAL	EDP FILES	EDP DATA	EDP PROGRAMS

- Place a cross in the appropriate box.

#### 6.4 Assets risks

Based on Figure 6M, prepare a spreadsheet (Figure 6) to summarise assets by location or program in rows against types of assets in columns. Place a dollar value on the types of assets to help identify your exposure.

Assets that present opportunities for personal use are: real estate, farms, domestic accommodation, mobile equipment, transport equipment, special processing facilities, portable and attractive items, very high value and unique items, on-loan equipment, confidential or sensitive information and staff time. Smaller items are more vulnerable to theft or removal by staff, clients or suppliers.

Your organisation should have a complete, up-to-date assets register, and the assets should be randomly audited.

#### 6.5 Risks for liabilities and obligations

You might also prepare a spreadsheet of your liabilities by location or program (rows) and type (columns) to complete your financial picture. This information will not be required by all organisations. A sample spreadsheet is not provided here.

#### 6.6 Summary

Spreadsheets provide an overview of the potential financial risk areas faced by your organisation. They can also be adapted to provide an overview of non-financial aspects.

The next step is to look more closely at your exposure to risks, which will allow you to select the "most exposed" for further attention.

**FIGURE 6M**

### FINANCIAL DIMENSION OF ASSETS (\$million)

[illegible]

- Place a dollar amount in the appropriate box.

### FINANCIAL DIMENSION OF ASSETS (\$million)

[illegible]

- [illegible]



## 7. THE RISK PROFILE

A risk profile describes your organisation's potential for loss through corruption.

The spreadsheets you completed for revenue, expenditure, resources and liabilities can all be adapted to risks.

Using the financial without risk factors spreadsheets, select those items you judged to be exposed to corruption. You will now prepare spreadsheets to focus on the *risk* areas in which corruption could take place:

- Revenue (Figure 7)
- Expenditure (Figure 8)
- Assets (Figure 9)
- Resources (Figure 10)

These spreadsheets list the elements at risk in rows (e.g. special funds) and the type of risk in the columns (e.g. theft). For a more detailed analysis, insert a cross in the active cell. In the active cells, enter a number or alpha code that refers to a separate description of the exposure (condition), risk (loss) or control.

Exposure to corruption is analysed as *potential* – or *inherent* – risk. This is the corruption which can strike if there is no control in place. By considering corruption in this way, you can assess the full potential loss and all the causal factors. The nature and effectiveness of the controls are considered separately.

At a later stage you should consider the *residual* risk to the organisation after a control is applied. If this level of risk is still unacceptable, further controls will be required.

### 7.1 Known corruption incidents

Experience is the starting point for any risk analysis and provides a reference for source, type and control. Use Figure 11 to take actual cases of corruption and score them within a high or low risk category. This will allow you to learn from others who have experienced similar or different types of corruption and ensure that all your potential risks are identified.

### 7.2 Organisational objectives

Your review should also identify risks that can impair the achievement of your program objectives.

Linking objectives with funds is part of the budget preparation process and will provide the categories for the 'objectives' column in Figure 12. For example, a roads and traffic authority might have an objective that gives road safety high priority. A feature of the program will be driver education and testing, yet the licensing branch could be corrupt and issue some licences without fully observing the qualifying criteria. In another case, a meat industry agency might want to promote the quality of its products. If, however, one producer is found substituting poor quality meat for premium grade, the credibility of the whole industry could be destroyed.

Generic financial risks were covered in section 6.5. You can now place these risks against the organisation's revenue, expenditure, assets and resources. Summarise the objectives on a spreadsheet in rows (e.g. levy collection) and the risks (e.g. theft) in columns (see Figure 12). Those cells marked as active indicate that a risk applies to an objective or a resource.

On a separate sheet, you can record the exposure to risks in more detail, then compare them with other corruption risks.

**FIGURE 7M ANALYSIS OF RISK TO REVENUE**

NO. PROGRAM REVENUE	THEFT	UNDUE INFLUENCE	NEGLECT OF DUTY	MISUSE OF RESOURCES	INVALID INFORMATION	FORGED INFORMATION
Government Appropriate	X	X	X	X	X	X
Special Funds			X	X	X	
Program Levies			X			
Licence Fees			X		X	X
Industry Subs						
Sales						
Service						

- Place a numeric or alpha code in the appropriate box. See section 8.

**FIGURE 7**

**ANALYSIS OF RISK TO REVENUE**

NO. PROGRAM REVENUE	THEFT	UNDUE INFLUENCE	NEGLECT OF DUTY	MISUSE OF RESOURCES	INVALID INFORMATION	FORGED INFORMATION
Government Appropriate						
Special Funds						
Program Levies						
Licence Fees						
Industry Subs						
Sales						
Service						

- Place a numeric or alpha code in the appropriate box. See section 8.

**FIGURE 8M ANALYSIS OF RISK TO EXPENDITURE**

NO. PROGRAM EXPENDITURE	WRONG SUPPLY	UNDUE INFLUENCE	NEGLECT OF DUTY	BRIBERY	INVALID INFORMATION	FORGED INFORMATION	UNAUTHORISED ACTIONS
Local Govt. Allocation		X	X		X		
Special Funds			X		X		X
Program Benefits			X				
Grants (incl. R & D)	X	X	X	X	X	X	
Program Supplies	X		X				
Salaries			X			X	X
Admin. Supplies	X	X		X			

- Place a numeric or alpha code in the appropriate box. See section 8.

**FIGURE 8****ANALYSIS OF RISK TO EXPENDITURE**

<b>NO. PROGRAM EXPENDITURE</b>	<b>WRONG SUPPLY</b>	<b>UNDUE INFLUENCE</b>	<b>NEGLECT OF DUTY</b>	<b>BRIBERY</b>	<b>INVALID INFORMATION</b>	<b>FORGED INFORMATION</b>	<b>UNAUTHORISED ACTIONS</b>
Local Govt. Allocation							
Special Funds							
Program Benefits							
Grants (incl. R & D)							
Program Supplies							
Salaries							
Admin. Supplies							

- Place a numeric or alpha code in the appropriate box. See section 8.

**FIGURE 9M ANALYSIS OF RISK TO ASSETS**

NO. PROGRAM ASSETS	VALUE \$m	THEFT	NEGLECT OF DUTY	BRIBERY	MISUSE OF RESOURCES	MALICIOUS DAMAGE	UNAUTHORISED ACTIONS
Land	6				X	X	
Buildings	30		X		X	X	X
Production Equipment	13	X			X	X	
Mobile Equipment	17	X	X		X	X	X
EDP Equipment	7	X	X	X	X	X	X
Stock	5.5	X	X	X			X
Debtors	2.5		X	X			X
SUMMARY	81						

- Place a numeric or alpha code in the appropriate box. See section 8.

**FIGURE 9**

**ANALYSIS OF RISK TO ASSETS**

NO. PROGRAM ASSETS	VALUE \$m	THEFT	NEGLECT OF DUTY	BRIBERY	MISUSE OF RESOURCES	MALICIOUS DAMAGE	UNAUTHORISED ACTIONS
Land							
Buildings							
Production Equipment							
Mobile Equipment							
EDP Equipment							
Stock							
Debtors							
SUMMARY							

- Place a numeric or alpha code in the appropriate box. See section 8.

**FIGURE 10M ANALYSIS OF RISK TO RESOURCES**

NO. PROGRAM ASSETS	THEFT	UNDUE INFLUENCE	NEGLECT OF DUTY	BRIBERY	MISUSE	MALICIOUS DAMAGE	UNAUTHORISED ACTIONS
Assets	X				X	X	
Finance/Funds	X		X		X		X
Staff		X	X	X			X
External Relationships	X						X
Information							

- Place a numeric or alpha code in the appropriate box. See section 8.

**FIGURE 10 ANALYSIS OF RISK TO RESOURCES**

NO. PROGRAM ASSETS	THEFT	UNDUE INFLUENCE	NEGLECT OF DUTY	BRIBERY	MISUSE	MALICIOUS DAMAGE	UNAUTHORISED ACTIONS
Assets							
Finance/Funds							
Staff							
External Relationships							
Information							

- Place a numeric or alpha code in the appropriate box. See section 8.



**FIGURE 11M ANALYSIS OF KNOWN CORRUPTION RISKS**

CORRUPTION RISKS TO PROGRAMS	KNOWN CASES	RATING SCORE	COMMENTS
Theft	6	4	
Wrong Supply	33	5	
Malicious Damage	16	4	
Bribery	1	1	
Undue Influence		1	
Neglect of Duty	7	2	
Unauthorised Actions	24	4	
Misuse Resources	12	2	
Invalid Information	73	5	
Forgery	2	1	
SUMMARY RISK			

- Place numbers in 'known cases' column. Place rating score in the high-risk and low-risk columns. Low risks 1 - 3, high risks 4 - 5.

**FIGURE 11 ANALYSIS OF KNOWN CORRUPTION RISKS**

CORRUPTION RISKS TO PROGRAMS	KNOWN CASES	RATING SCORE	COMMENTS
Theft			
Wrong Supply			
Malicious Damage			
Bribery			
Undue Influence			
Neglect of Duty			
Unauthorised Actions			
Misuse Resources			
Invalid Information			
Forgery			
SUMMARY RISK			

- Place numbers in 'known cases' column. Place rating score in the high-risk and low-risk columns. Low risks 1 - 3, high risks 4 - 5.

**FIGURE 12M**

**ANALYSIS OF RISK TO THE ORGANISATION'S OBJECTIVES OR PROGRAMS**

ORGANISATION ELEMENTS AT RISK	THEFT	WRONG SUPPLY	MALICIOUS DAMAGE	BRIBERY	UNDUE INFLUENCE	NEGLECT OF DUTY	UNAUTHORISED ACTIONS	MISUSE RESOURCES	INVALID INFORMATION	FORGERY	SUMMARY RISK
OBJECTIVES											
PROGRAM ACTIVITIES Levy Collection Benefits & Grants Licensing & Registration Construction Administration						x x x	x	x	x		
PHYSICAL RESOURCES Program Equip Portable & Attractive	x x		x x			x	x	x x			
FINANCIAL RESOURCES Bank Balances Investments	x x			x	x	x x	x x	x			
HUMAN RESOURCES Management Remote Location Staff				x	x x	x x	x				
INFORMATION Sensitive Confidential	x x	x		x x	x x	x x	x x		x x	x x	
CLIENTS Data Dependent Benefit Recipients		x		x	x				x x	x x	
SUPPLIERS Expertise Dependent Remote Location Delivery	x x x	x x	x	x x x	x x x		x x x			x x	
SUMMARY RISK											

- Place a numeric or alpha code in the appropriate box.

**FIGURE 12 ANALYSIS OF RISK TO THE ORGANISATION'S OBJECTIVES OR PROGRAMS**

ORGANISATION ELEMENTS AT RISK	THEFT	WRONG SUPPLY	MALICIOUS DAMAGE	BRIBERY	UNDUE INFLUENCE	NEGLECT OF DUTY	UNAUTHORISED ACTIONS	MISUSE RESOURCES	INVALID INFORMATION	FORGERY	SUMMARY RISK
OBJECTIVES											
PROGRAM ACTIVITIES Levy Collection Benefits & Grants Licensing & Registration Construction Administration											
PHYSICAL RESOURCES Program Equip Portable & Attractive											
FINANCIAL RESOURCES Bank Balances Investments											
HUMAN RESOURCES Management Remote Location Staff											
INFORMATION Sensitive Confidential											
CLIENTS Data Dependent Benefit Recipients											
SUPPLIERS Expertise Dependent Remote Location Delivery											
SUMMARY RISK											

- Place a numeric or alpha code in the appropriate box.

## 8. ASSESSING CORRUPTION RISKS

Once you have identified the risks, you need to assess their severity and determine the appropriate level of control. It simply may not be economical or efficient to impose elaborate controls over low risk areas or low value assets. The form of assessment will vary, depending on how much you know about the risk.

For a large-scale risk, such as false overtime claims or the stealing of computers, VCRs, and TVs, statistics may suggest a pattern. If you can predict how, where and by whom offences would be committed, you can then design an effective ticketing system and deploy inspectors to the maximum benefit.

The assessment of unusual or isolated risks is limited by a lack of data. There are options, but they all depend on subjectivity to some extent:

- comparative risk ranking, by an expert group, according to selected criteria
- seeking feedback via a survey, then scoring and weighting the results on a relative scale
- scoring nominated risk factors
- judging on a scale of high, medium and low corruption according to established criteria.

### 8.1 Ranking the assessment of corruption risks

Before you can decide what level of control is needed for a particular risk, you must calculate the relative frequency, costs and severity of incidents. High frequency/high severity risks must be strongly controlled, while low frequency/low severity risks require less control. High frequency /low severity risks and low frequency/high severity risks occupy the middle ground.

To keep the assessment simple use a high (H), medium (M), and low (L) scale.

Making assessments should be a team effort. It can be coordinated by a risk assessment committee, but the person in charge should work closely with the program/activity managers. Your approach is determined from the spreadsheet analyses and from the risks you identify as relevant to particular programs/activities.

The risks should be discussed with the program/activity managers. The analyst's "feel" for the potential risks and the manager's familiarity with the area provide a basis for the assessment.

You can then prepare a summary spreadsheet showing the high, medium or low (H/M/L) ranking in the active cells (see Figures 13M/13). Tabulate high risks from all programs, then group similar elements at risk from different programs. Compare the rankings to make sure that a high ranking has not been unfairly awarded to a particular risk.

Any disagreement between assessors should be addressed by the risk assessment committee. Consistency should be the goal.

### 8.2 Assessment of high corruption risks

One method of assessing risks is to analyse forms of corruption in terms of

- incentive
- opportunity
- concealment
- prevention difficulty
- detection difficulty
- diminished ethics.

#### 8.2.1 Incentive

Incentive can be calculated as the amount or benefit the offender would be likely to gain. The type of crime, personal circumstances and ethical standards of the client may vary the level of risk.

#### 8.2.2 Opportunity

The risk increases if you rely on the client or supplier for data without a checking procedure. The opportunity for corruption increases where operations are inefficient, staff are uninterested and control practices are weak.

### **8.2.3 Concealment**

A supplier or client may be able to conceal the true nature of the services or information provided. After an activity is completed, it may be difficult to verify the details, especially if it takes place at a remote location. Employees who understand the control system are better able to conceal corrupt behaviour.

### **8.2.4 Prevention difficulty**

It may be hard to prevent corrupt activity by a supplier if your organisation lacks the expertise to set a standard for a technical specification for a product or service. It is also difficult to prevent corruption by managers who breach positions of trust and use their authority to conceal the acts.

### **8.2.5 Detection difficulty**

It is also sometimes difficult to detect corruption. It is difficult to know if a representative has negotiated hard enough for the organisation, and, if not, if this constitutes neglect of duty. When portable equipment "goes missing" it may be difficult to know if it was stolen, when and by whom.

### **8.2.6 Diminished ethics**

Informal networks may indicate that some areas have entrenched pilferage, and false claims may be "normal practice", but the extent to which ethics has diminished in an organisation may be difficult to assess. Even when evidence is available, the risk of defamation actions makes it dangerous to accuse employees, clients or suppliers.

**FIGURE 13M**

**ASSESSMENT OF HIGH RISK ATTRIBUTES**

RISK SOURCE	THEFT	WRONG SUPPLY	MALICIOUS DAMAGE	BRIBERY	UNDUE INFLUENCE	NEGLECT OF DUTY	UNAUTHORISED ACTIONS	MISUSE OF RESOURCES	INVALID INFORMATION	FORGERY	SUMMARY RISKS
Incentive		M	M	L		L	M	L		L	
Opportunity	H	M	H	L		M	H	L		L	
Concealment				L			M				
Prevention Difficulty	H	M	H	H		M	H		H	H	
Detection Difficulty		H	M	H		L	M	M	H	H	
Diminished Ethics	M	H		L		M					
Others											
SUMMARY RISK											

- Place a H, M or L in the appropriate box.

**FIGURE 13** **ASSESSMENT OF HIGH RISK ATTRIBUTES**

RISK SOURCE	THEFT	WRONG SUPPLY	MALICIOUS DAMAGE	BRIBERY	UNDUE INFLUENCE	NEGLECT OF DUTY	UNAUTHORISED ACTIONS	MISUSE OF RESOURCES	INVALID INFORMATION	FORGERY	SUMMARY RISKS
Incentive											
Opportunity											
Concealment											
Prevention Difficulty											
Detection Difficulty											
Diminished Ethics											
Others											
SUMMARY RISK											

- Place a H, M or L in the appropriate box.



## 9. A SIMPLIFIED RISK ANALYSIS PROCEDURE

Success at corruption prevention depends on the resources available for risk assessment. Smaller organisations may not have the resources, staff or skills to carry out a complex procedure. For such organisations, a simplified model may be just as effective.

The following section deals with the roles of the key players in a simplified corruption risk analysis program.

### 9.1 The key players and their roles

Senior managers

- determine resources and practices
- define the expected outcomes from the risk analysis
- encourage support for the analysis
- apply suitable resources to the assignment, for example, staff, materials, other internal staff, other agencies and consultants.

Risk analysts

- set up the project's scope, planning and consulting with senior managers and users
- explain the project objectives to all managers and staff
- collect data
- identify corruption exposures, sources, elements at risk, and losses
- develop an acceptable risk rating and ranking methodology
- assess the risks
- evaluate prevention and detection controls.

### 9.2 The model

The four major elements are:

- scope
- identification
- evaluation
- control.

### 9.3 Scope

Determining the scope of the project will help you decide how your organisation can be divided for assessment. Use categories like financial and non-financial systems, programs, organisational structure or physical location. You should also consider factors such as the organisation's size, its geographical distribution and the resources available for the assessment.

### 9.4 Identification

Refer to section 4 for a list of generic types of corruption, a profile of corruption risks and potential sources of corruption.

Identify how these risks might affect your organisation, then, after referring to Figure 14M, collate the details in Figure 14. In the first column list the area being assessed. In the second, list the associated risks you have identified.

### 9.5 Evaluation

Evaluate the risks by considering

- how likely it is that an incident will occur
- the consequences to the organisation
- the seriousness of the consequences.

On the basis of these factors, estimate the risk as high, medium or low. Enter these rankings on the worksheet. You can then decide what, if anything, needs to be done to lessen the risk.

In summary, ask yourself, *What is it about the organisation's current way of operating that stops it from going off the rails?*

## 9.6 Control

Figure 14 asks you to

- identify risks associated with areas you are assessing
- evaluate those risks and the controls already in place
- consider how the current controls might be improved.

Consider whether the controls are sufficient to prevent or detect the risk. If the risk is high and

the controls are inadequate, what improvements will provide adequate control? If there are costs implications, balance these against the level of risk and the consequences of inaction. This will provide you with an acceptable control. Enter this in the Control Improvement column.

You will prepare your control plan from this column (see section 12).

List the controls and a strategy for their implementation, including who will be responsible for implementation and by what deadline. If several controls are needed you may have to prioritise them.

**FIGURE 14M**                      **SIMPLE RISK ASSESSMENT WORKSHEET**

IDENTIFICATION		EVALUATION		CONTROL	
AREA BEING ASSESSED	ASSOCIATED RISKS	RISK HIGH, MEDIUM OR LOW	IDENTIFIED CONTROLS	CONTROL IMPROVEMENTS	
Dalby workshop	Theft of stock	H	Locked doors Branding stock	Key register Banning private vehicle access After hours security patrols	
	Mis-use of equipment	M	Asset register	Physical security and supervision. Policy for loan	

• See section 9.6 - Control.

**FIGURE 14**      **SIMPLE RISK ASSESSMENT WORKSHEET**

IDENTIFICATION		EVALUATION		CONTROL
AREA BEING ASSESSED	ASSOCIATED RISKS	RISK HIGH, MEDIUM OR LOW	IDENTIFIED CONTROLS	CONTROL IMPROVEMENTS

• See section 9.6 - Control.

## 10. DETAILED RISK ANALYSIS PROCEDURES

This section provides detailed risk analysis strategies for complex organisations that require a more sophisticated procedure.

Rather than attempt to assess every element, large organisations must decide what level of risk is acceptable, given their resources. Weigh the cost of resources you will need for effective control against the benefits such controls would provide. Summarise the extent of risk elements in your organisation by completing the spreadsheets that follow. You may then decide to analyse the risks comparatively.

### 10.1 Summary analyses

The spreadsheets should help if you are undertaking a risk analysis for the first time. They enable you to group risks under program activities and then evaluate your strategies for controlling them. Most of the spreadsheets are preceded by a model to help you develop your analysis.

In Figure 15 set organisational elements against particular risks then score the risks as high, medium or low.

Figure 16M shows the exposure, risk and controls for one important activity. Following the model, make enough copies of Figure 16 to cover all activities in your organisation that are exposed to corruption.

Figure 17M compares the controls in Figure 16M with the present procedures. In Figure 17, indicate if improvement is possible and identify the level of risk.

In Figure 18, describe in greater detail what control improvements are needed.

In Figure 19, summarise the effectiveness of control for each element you listed in Figure 18, noting if improvement is possible and the risk rating. Summarising each program element in the far right-hand column and each risk type in the bottom row will give you an overall assessment for programs and risk types.

**FIGURE 15**

<b>RISK ANALYSIS SUMMARY</b>											
<b>ORGANISATION ELEMENTS AT RISK</b>	<b>THEFT</b>	<b>WRONG SUPPLY</b>	<b>MALICIOUS DAMAGE</b>	<b>BRIBERY</b>	<b>UNDUE INFLUENCE</b>	<b>NEGLECT OF DUTY</b>	<b>UNAUTHORISED ACTIONS</b>	<b>MISUSE RESOURCES</b>	<b>INVALID INFORMATION</b>	<b>FORGERY</b>	<b>SUMMARY RISKS</b>
<b>PROGRAM ACTIVITIES</b> Levy Collection Benefits and Grants Licensing & Registration Construction Administration											
<b>PHYSICAL RESOURCES</b> Program Equipment Portable & Attractive											
<b>FINANCIAL RESOURCES</b> Bank Balances Investments											
<b>HUMAN RESOURCES</b> Management Remote Location Staff											
<b>INFORMATION</b> Sensitive Confidential											
<b>CLIENTS</b> Data Dependent Benefit Recipients											
<b>SUPPLIERS</b> Expertise Dependent Remote Location Delivery											
<b>SUMMARY RISK</b>											







**FIGURE 17M ANALYSIS OF PRESENT CONTROLS AND POTENTIAL FOR IMPROVEMENT**

INDICATIVE CONTROL (Refer to Figure 16M)	PRESENT CONTROL PROCEDURE	IMPROVE? Y/N	RISK H-M-L
FINANCIAL			
POLICY			
COMPUTING Password Security Testing for Viruses	Written request. No update policy. Ad hoc control.	Y Y	H H
INTERNAL Physical Security	Keys issued.	Y	M
EXTERNAL			
SUMMARY			

**FIGURE 17 ANALYSIS OF PRESENT CONTROLS AND POTENTIAL FOR IMPROVEMENT**

INDICATIVE CONTROL (Refer to Figure 16M)	PRESENT CONTROL PROCEDURE	IMPROVE? Y/N	RISK H-M-L
FINANCIAL			
POLICY			
COMPUTING			
INTERNAL			
EXTERNAL			
SUMMARY			





## ANALYSIS SUMMARY OF CONTROLS

67

## FIGURE 19

PROGRAM CORRUPTION EXPOSURE (Refer to Figure 18)	CONTROL STATUS: IMPROVE? (Y/N) RISK (Y/N)					
	FINANCIAL	POLICY	COMPUTING	INTERNAL	EXTERNAL	SUMMARY
Password Security						
Testing for Viruses						
Physical Security						
SUMMARY CONTROL STATUS						

## 10.2 Comparative ranking

In some cases you may then decide to compare and rank the risks you have identified. This procedure is particularly useful in large decentralised organisations.

Risk categories are assessed by a small group of people who know and are responsible for the particular area. This group, known as a *Delphi team*,

- controls the analysis of results
- determines the most appropriate criterion against which to compare the risks
- ranks the risks.

Risks are paired, and team members vote for the risk they perceive to be the greater. The sum of their votes provides the ranking. A wide spread in the scores can indicate relatively high or low risks. For example, if theft is always regarded as a higher risk than other corrupt activities, it should be ranked the highest.

The method is even more efficient if Rank-It software is used. Rank-It is a low-cost package produced by Jerry FitzGerald & Associates, which provides a ranking worksheet, accepts scores, calculates rankings and prints a ranked list.

## 10.3 Questionnaire-based methods

A *questionnaire* can help assess the risks of a decentralised organisation uniformly. Its scope must be carefully determined by the risk assessment committee.

Designing and administering a questionnaire need not be a drain on resources. Staff who participate should be thoroughly briefed and encouraged to have some sense of ownership. A support hot line can be set up to provide more information and assessment.

The committee should apply different weights to risks to reflect the concerns of particular programs and the sensitivity or value of the relevant element. To compare the level of risk for each program, the weighted risks are then scored on a single scale such 1-3, 1-5 or 1-10, from lowest to highest risk.

In applying the questionnaire method, the risk committee should ensure that it

- develops appropriate questions
- links the questions with the model
- structures the model to produce relatively ranked risks.

A *risk-scoring* model can also be developed. A spreadsheet can be designed to summarise factors that indicate risks, the elements at risk and the control systems. Several factors can be selected for assessment. Program managers should be actively involved in selection and scoring to ensure their support. You will need at least six to eight significant risk factors to develop a useful ranking. Beyond that number, the relative ranking between units is unlikely to change merely by introducing more factors.

A spreadsheet is prepared for each program or location. The risks are assessed from lowest to highest, with a known incident rating 10, and a high risk rating 20.

## 11. CORRUPTION PREVENTION AND CONTROL PRACTICES

Managers need to design or develop a control system that best meets the specific circumstances of their individual programs. There are several factors to be considered before the system can be implemented.

### 11.1 Corporate ethos and practice

Managers can encourage, or even prescribe, acceptable behaviour but should not expect compliance without the support of a sound corporate ethos. Staff are unlikely to support a control system unless they have been involved in its formulation and implementation.

There are four aspects that you should consider:

1. A clear policy on corrupt behaviour by employees must be seen to be initiated and supported by senior management. Experience has shown that organisations cannot rely on the adequacy of general prohibitions on corruption (which apply to all public sector agencies) to have an impact on a specific workplace.
2. To have the intended deterrent effect, policies must be actively disseminated to all staff. Education and training programs must reinforce the point that corrupt behaviour will never be sanctioned. Operational standards must also consistently reflect the policy.
3. Disciplinary measures spelt out in the policy must be put into practice. Further, the policy must be applied equitably. If senior staff are treated differently from junior members, this will greatly erode the sense of fairness necessary to prevent corruption.
4. There are two types of deterrents – specific and general. If corrupt activity is covered up, it does little to deter others.

To be a deterrent, actions against corrupt staff must be made public. Announcing that unnamed employees have been prosecuted or disciplined for corrupt behaviour will encourage other staff to calculate realistically the risks of getting caught and lessen the chances of further corruption.

Consider the following to determine whether your organisation adequately addresses corruption in the workplace:

- Does your organisation possess a formal written policy or does it have rules prohibiting employee corruption? Is this widely known by staff?
- Are new staff made aware of this policy during orientation?
- Is the policy disseminated to all staff or only to certain groups?
- Is the topic of employee corruption covered in forums other than orientation, for example, in newsletters or on bulletin boards?

### 11.2 Management attitude

The attitude of managers sets the standard for staff to follow and is critical to the success of any control system. Senior managers should send positive corruption prevention messages. Negative messages may invite staff to become lax in their attitude towards controls.

Here are some examples of negative messages:

- suggesting that the ability to “get the job done” and “the end justifying the means” are the major criteria for staff advancement
- stressing the meeting of budgets and deadlines over integrity
- creating strong management controls but not monitoring for compliance
- ignoring complaints from clients or staff
- failing to investigate over-rides of controls by managers
- communicating with staff from the top down



- ignoring the personal problems of staff in positions of responsibility.

Supervisors are expected to ensure that behavioural standards are maintained in the workplace. They also interpret the rules that govern their work groups. The manner in which a supervisor chooses to implement a plan is a relatively reliable indicator of the standards against which staff behaviour will be measured.

In a sense, supervisors barter flexibility or permissiveness in the workplace to encourage co-operation from their staff. One supervisor, asked about management policy in corruption prevention, responded:

Management sit down and write the policy they think is necessary to accomplish the things they want to accomplish. As supervisors, we take what they have written and interpret it in our own way. We cannot treat people like robots and say such things as "If you're a minute late, you'll be written up for being a minute late," or "You have been late three times so you will be disciplined." We take management's strict rules and plug them into our own atmosphere in a way that we feel is right and that will get the job done effectively.

A similar process applies in most organisations. Dynamic corruption prevention is the means by which supervisors mediate between rules, including those in a corruption prevention plan, and the day-to-day requirements of the unit. Supervisors must be convinced of the value of corruption prevention and clearly understand the negative impacts of corrupt activity on the organisation's efficiency. They should also realise that corruption discovered in their area will reflect poorly on their competence.

### **11.3 Staff involvement**

Competent, trained, trustworthy staff are essential to corruption prevention. Managers and supervisors should assess the trustworthiness of applicants for positions. The more sensitive the position, the closer the scrutiny must be.

The Public Sector Management Commission has issued standards on staff selection and human resource management. Of particular relevance to corruption prevention are:

- recruitment and selection

- performance planning and review
- executive performance management and development
- fair treatment of employees
- managing diminished performance
- position descriptions.

If staff feel that their contributions are not appreciated, or that management is indifferent to corruption, corrupt activity will increase. On the other hand, when managers are responsive to the perceptions, attitudes and needs of staff, corruption decreases.

## **11.4 Key control elements**

The following are key elements crucial to a cost-effective reduction of the risks in any organisation.

### **11.4.1 Effective supervision**

Effective and sensitive guidelines can help supervisors and staff deal with suspect or aberrant behaviour. Managers should monitor activities by means of system reports and random checks. Shortfalls in performance should be reviewed for possible corruption.

### **11.4.2 Adequate authorisation procedures**

Authorisation links senior employees to transactions and activities they carry out and provides an audit trail.

In the public sector, more authority is being given to junior staff, with second-level approvals becoming less common. Senior managers must monitor how delegates exercise this authority and should also set up timely review procedures.

### **11.4.3 Segregating conflicting duties**

Segregating conflicting duties is a standard control against corruption. It is unreasonable to expect that staff will always resist temptation if they have both access and opportunity to become involved in corrupt practices and the opportunity to cover up their activities.

In smaller organisations it is not always possible to segregate duties. Cost pressures might require combining some tasks. In such cases, a compensating control measure should be applied. Reviews of high-value transactions and random checks are essential.

#### **11.4.4 Safeguards against conflicts of interest**

People with special responsibilities who work without close supervision must declare conflicts of interest. The declaration should require them to state any conflict between their job and private interests.

All staff should be audited regularly to ensure that undeclared conflicts of interest are identified.

#### **11.4.5 Well-defined transaction procedures**

Procedures that are well-defined ensure that records and forms contain all the required information to describe a transaction, particularly when they apply to applications for a licence, registration or a grant. The completion of the form then becomes part of the control.

#### **11.4.6 Data and management information systems security**

Data and management systems security is essential for effective corruption control. The accuracy of reports on program activities, financial transactions and their status depend on data and system integrity. Data and their method of processing must be accurate, complete, timely, authorised and as far as possible tamper-proof.

Numeric accuracy is an obvious corruption-related control. Recording transactions and processing records completely ensures that system data represent the total picture.

Efficient data control requires prompt processing of records and knowing the status of outstanding transactions. Properly authorised and processed data add to the control process.

Data files must be protected. Restricting access limits opportunities for manipulation.

#### **11.4.7 Physical security over assets**

Physical security for assets is basic to corruption prevention. The level of security depends on the importance of the asset and the access needed for operations. The level of control needs to be proportional to the potential risk.

#### **11.4.8 Independent review of controls**

Independent reviews evaluate the effectiveness of controls. An internal audit is one control in the prevention and the detection of fraud.

Give your internal auditors a wide brief and ask them to focus on corruption risks and their possible control.

Internal audits are sometimes limited to occasional visits and selective reviews and an internal audit might not detect corruption if transaction tests are not sufficiently broad or rigorous. You therefore must

- ensure the audit provides an appropriate level of prevention
- recognise that your managers, not the auditors, are principally responsible for corruption control.

Corruption prevention controls must be analysed independently. This means being outside the audited area and free from undue influence or "blind spots". Ensuring independence can help you break up the aggregation of conflicting duties.

### **11.5 Analysis of controls**

Figure 20 displays how controls apply to commonly identified risks. For each risk relevant to your organisation apply a risk level (H-M-L) and a current control effectiveness rating (H-M-L). For example, if your organisation is highly vulnerable to theft and managers are lax in their attitude toward detecting it, you would enter H/L in the appropriate box and identify this as a high priority area for preventative and control measures.

**FIGURE 20** ANALYSIS OF THE EFFECTIVENESS OF CONTROLS

RISK CONTROL	THEFT	WRONG SUPPLY	MALICIOUS DAMAGE	BRIBERY	UNDUE INFLUENCE	NEGLECT OF DUTY	UNAUTHORISED ACTIONS	MISUSE OF RESOURCES	INVALID INFORMATION	FORGERY	SUMMARY RISK
Management Attitude											
Corporate Ethos											
Competent Staff											
Performance Standards											
Monitoring Systems											
Supervision											
Authorisation											
Segregation of Duties											
Declaration of Interests											
Sound Procedures											
Data Integrity											
Physical Security											
Independent Review											
Other											
SUMMARY RISK											

## 12. DESIGN AND EVALUATION OF CORRUPTION PREVENTION CONTROLS

Once you have considered the nature of the program activity, identified the potential types of corruption and recognised the resources at risk, you should then select relevant and effective controls.

Internal auditors can offer advice but should not design systems because this might diminish their independence and objectivity.

The control system should be documented to ensure that staff are trained and competent in any new procedures.

After a trial period, check the effectiveness of the control system. Based on your review and feedback from staff, you may decide to modify your procedures.

Internal audit should also evaluate the control system. Auditors can clarify the purpose of the system and identify the expected standards of performance. Internal auditors should also encourage staff to suggest improvements, which can then be discussed with managers. Auditors should use a standard format to interview managers and staff. This will ensure that the important issues are covered and that data are collected and summarised consistently.

Samples of general and special risk analyses follow. The examples indicate the kind of data that can be collected to guide organisations in designing their own evaluation forms.

The design of corruption prevention controls should include

- a checklist of potential problem issues
- methodical risk analysis and corruption control tables.

It is essential to

- identify resources or activities susceptible to corruption
- realistically assess the seriousness and degree of risk
- identify and assess current corruption controls
- identify and implement appropriate corruption controls.

Figure 21 is a general survey form suitable for most program activities. The headings describe the management framework and risk features of the program or activity. The analysis then becomes the basis for your evaluation and improvement of controls.

**FIGURE 21****PROJECT:** \_\_\_\_\_

MANAGEMENT FRAMEWORK	CORRUPTION RISK ANALYSIS
Objectives	Exposures
Standards	Risks
Performance Measures	Control
Monitoring Systems	Risk/Control Payoff

Figure 22 is an example of a single-page report, summarising corruption risks, conditions and controls covering income, expenditure, resources and information for a program.

**FIGURE 22****PROJECT:** \_\_\_\_\_

POSSIBLE CORRUPTION RISK	CORRUPTION CONDITION	CORRUPTION CONTROL
Income <ul style="list-style-type: none"> <li>Fully invoiced</li> <li>Collected</li> </ul>		
Expenditure <ul style="list-style-type: none"> <li>Quality</li> <li>Quantity</li> <li>Actually received</li> <li>Received on time</li> <li>Proper price</li> </ul>		
Property, Equipment and Stock <ul style="list-style-type: none"> <li>Secure access</li> <li>Proper use</li> <li>Ready for use</li> </ul>		
Information <ul style="list-style-type: none"> <li>Accurate</li> <li>Secure access</li> <li>Secure release</li> </ul>		

### 12.1 Can there be too much control?

Deciding how much control should be exercised is not easy. Before implementing controls you must balance the costs of introducing controls against the benefit.

Consider the impact of controls on supervisors' workload and productivity. Controls that impose on supervisors may also be perceived by staff as diminishing the level of trust placed in them.

Controls should not take the form of rules and obligations that discourage responsible judgment and discretionary power. Controls enforced without rationality, need or consideration for the staff affected by them can lead to resistance or petty acts of fraud or theft.

In assessing the control costs you should consider

- the number of persons required under Finance Regulations to ensure regularity of expenditure and receipt of public moneys does not constitute 'over-control' relative to amounts received and expended
- whether or not the scope and capacity of computerised equipment used to process management information and accounting documents and records is excessive
- activities that may be redundant or at least marginal in value, such as
  - the use of human and physical resources for the protection of assets which may be at risk, e.g. determine the alternative cost of insurance
  - extent of the employment of duplicate systems, records and staff to reduce errors in records and operations
  - more effective use of internal audit to reduce control costs including costs of external audit and consultancies.

### 12.2 Overcoming resistance to controls

Before implementing controls, managers should

- make sure that their goals, objectives and standards are realistic
- involve those employees who will be bound by them
- install controls only when necessary for prudent management, and periodically consider if they are still needed or require refinement
- ensure that the administration and monitoring of controls are delegated to junior as well as senior staff
- ensure that staff are aware of, and understand, the controls, and that surveillance is as unobtrusive as possible.

### 12.3 Implementing controls

Ask yourself the following questions.

*Is there effective control at the organisational level?*

Controls can include

- a comprehensive organisational chart
- an organisational chart covering all activities and providing for unambiguous lines of authority, responsibility and decision making
- a management manual specifying, for all levels of responsibility, the duties, practices, procedures and specifications necessary for the control of operations
- regular reviews of organisational charts and manuals by senior managers, noting changes in departmental functions and governmental regulations
- systems properly documented and charted in formal systems manuals.

*Is there effective control at operational level?*

Controls can include

- an adequate management information system

- provision for reporting of variances between actual performance and budgets and standards
- evidence that variances are followed up by management and internal audit
- evidence that budgets and standards have been set to encourage efficiency rather than to be easily attainable.

*Is there effective control at a managerial level?*

Controls can include

- data collected to evaluate the organisation's services and the costs of activities
- statistics compiled for planning, specifically to revise activity levels and adjust the organisation's needs for resources
- regular reports to management on factors which materially affect the level and nature of services to be provided.

*Are management controls regularly reviewed?*

Controls can include

- internal audit or other monitoring functions
- planned revision dates.

*Are management attitudes towards controls appropriate?*

To address this question, an auditor might consider the following:

- Is responsibility for controls taken at the senior management level?
- Do senior managers delegate this responsibility satisfactorily? e.g. to auditors?
- Is there a policy for dealing with fraud when it is discovered or suspected, concerning
  - notification of the CJC and the QPS
  - investigation arrangements

- discipline of employees
- involvement of auditors?

Are there arrangements to regularly communicate to management and staff

- the principal officers' attitude towards controls
- the policy for dealing with fraud and corrupt behaviour?

- Does the principal officer ensure that information received from managers is reliable and complete?
- Does the principal officer support the quality and independence of internal audit?
- Does the principal officer clearly demonstrate that he or she insists on high standards of corporate and individual behaviour?
- Do the organisational structure and arrangements for supervision support these high standards?
- Is segregation of duties adequate?
- Does the corporate culture support high standards and discourage fraud?

### **12.3.1 Physical security of assets**

The principal risk to assets is theft. Because many public sector organisations are large and people move around frequently, maintaining a high level of security is not always easy.

Controls can include

- making staff accountable for assets under their specific control
- providing physical security in sites, premises and work areas
- distributing personal identification and access keys
- ensuring asset records are complete and up-to-date.

Figure 23 provides a sample Asset Inventory Risk Assessment Control Planner.

**FIGURE 23 ASSET INVENTORY CORRUPTION  
RISK ASSESSMENT AND CONTROL PLANNER**

ASSET ITEMS	DESCRIPTION	RISK (H-M-L)	CONTROLS
Program Stocks			
Library			
Market Research Reports			
Merchandise			
Registry			
Stationery Supplies			
Technical Equipment and Components			
Maintenance Workshop			
Maintenance Spares			
Spare and Obsolete Equipment			
Personal Computers			
Portable and Attractive (List)			
Computer Files			
• Programs			
• Data			
Client/Supplier Equipment			
Equipment at Suppliers/Clients Premises			
Other			

An asset/inventory corruption control planning checklist could also include assessment of:

**Custody/Security**

- Access

**Identification**

- Tag/Label
- Status Record
- Stocktake

**Records**

- Complete
- Accurate
- Up-to-date
- Verified

**Utilisation**

- Authorised Issue
- Authorised Use
- Usage Records



### 12.3.2 Confidential information

Confidential information can involve sensitive decisions about future plans which might affect assets, personal details and commercially sensitive material. This information could be valuable to clients, external parties or could be considered newsworthy by the media. Staff could be tempted to release data for a fee or because of other motives.

Controls should include

- providing a code of conduct to cover confidential material
- having staff sign a declaration to maintain confidentiality
- ensuring custodians of information are sensitive to the risk of unauthorised disclosure
- keeping hard copy files physically secure
- restricting access to computer files
- ensuring staff know the penalties for release of confidential information.

### 12.3.3 Purchasing

All forms of purchasing have the potential for mismanagement, embezzlement, fraud and corruption. Purchasing procedures must seek value-for-money, ensure staff integrity and accountability, and guarantee equity to suppliers who wish to provide the goods or services.

To maintain equity, all prospective suppliers must be given the same information. When more information is provided in response to a candidate's request, or when a specification is extended or made more flexible, all candidates must be advised.

Controls should include

- implementing tender and quotation procedures for high-value purchases
- preselecting panels of suppliers, based on established and agreed criteria

- setting criteria for selecting and assessing the performance of suppliers, and establishing a procedure to collect and evaluate the appropriate data
- prescribing an evaluation procedure involving specialist staff from appropriate disciplines
- obtaining conflict of interest declarations from key staff.

Figure 24 provides a sample purchasing risk analysis and corruption control planning proforma.

**FIGURE 24**                      **CORRUPTION RISK ANALYSIS AND  
CONTROL PLAN/SELF EVALUATION EXAMPLE**  
**PROJECT PURCHASING AND PAYMENTS**

VALUE-FOR-MONEY CONTROLS	IMPORTANCE (1-10)	PERFORMANCE (0% - 100%)
<b>For Suppliers and Consultants</b> <ul style="list-style-type: none"> <li>Obtaining competitive quotations</li> <li>Setting performance criteria</li> <li>Reviewing quantities or time</li> <li>Evaluating performance</li> </ul>		
<b>Analysing Project Costs</b> <ul style="list-style-type: none"> <li>Commitment Advice (CA)</li> <li>Budget Control Reports (BCR)</li> </ul>		
<b>Recording in-kind contribution</b>		
<b>Evaluating Project Results</b> <ul style="list-style-type: none"> <li>For impact</li> <li>Value-for-money</li> </ul>		
<b>Other</b>		

**Importance (1-10)**

The importance of the control. Score 1-10, where 1 is high and 10 is low. Give each control a score from 1 to 10, depending on its importance. You may rate several controls as the same value, i.e., three controls may rate as 1 (highest importance).

**Performance (0% - 100%)**

Your current performance of the control. Score 0-100%, where 0% is no achievement and 100% is total effectiveness. Give each control the performance percentage you consider reflects your current performance, rather than what you might see as the desirable level of performance.

**Risk Control Factors**

Comment: The rationale for the scores used is to display the areas where high risks (low score) are under-controlled (less than 5). A risk control factor is determined by dividing the importance score by the decimal equivalent of the performance percentage. A high factor indicates a problem area.

**Control Improvements Needed:****Major Fraud Risk:**

#### 12.3.4 Contracts

Contracts can be corrupted in the same way as purchasing when value-for-money, integrity, accountability and equity objectives are not properly satisfied. In particular, contracts can be negotiated to favour one supplier. It can be difficult to prove corrupt behaviour in such cases, particularly if duties are concentrated in the negotiator.

Contracts with the potential for reciprocal payments can be used to identify contracts awarded to other than the lowest bidders. There are often genuine reasons, however, why the lowest price should not be accepted. Because of such factors as quality, service and supply continuity, the lowest *total* cost is not the same as the lowest *unit* cost.

Certain issues, like quality, economy and commercial terms, should be negotiated by people who specialise in, or who are responsible for, these elements. If specialists, purchasing staff and accountants are all involved in negotiations, conflicts in duties will be eliminated.

#### 12.3.5 The contract register

The risk of corruption in negotiations can be addressed by strict adherence to the tendering procedures and by establishing a contract register. While aimed at corrupt negotiators and suppliers, a contract register also allows purchasing officers to display integrity and equity and can support staff who have been wrongly suspected of corruption.

The contract register also addresses controls such as

- (real) quality and value-for-money expectations and budgetary accountability
- regular competitive review of supply criteria
- independent review of critical supply criteria
- conflict of interest policy, analysis and declarations

- independent authorisation of critical criteria and major, sensitive contracts.

For each contract, the register should specify

- date(s) – start and finish
- party(ies) involved
- the organisation's negotiator(s)
- product and/or service description
- quality, volume, service, cost, timing criteria
- total contract value
- quality assessment processes
- principal advantages of selected supplier
- other potential suppliers
- conflicts of interest (declared potential – who can influence and benefit?)
- supplier audit option
- date of last audit
- audit result (1 = OK; 2 = OK, but; 3 = not OK).

#### 12.3.6 Contract quotation evaluation

The following are crucial to an effective evaluation of quotations:

- adequate selection of suitable suppliers (define 'suitable')
- clear specification of key supply criteria
- effective measurement and comparison of offers
- verification of evaluation assumptions
- independent collection/evaluation of data
- visits to supplier (to verify any data provided).

**12.3.7 Travel allowances and expenses**

Exposure to corruption in this area depends on the accuracy of information supplied by staff.

Expenditures may be exaggerated or invented.

While most staff act with propriety, the elements of high risk (opportunity, incentive, low detection, high concealment) are always present.

Controls should include

- clear instructions about allowable expenses, with specific rules on the quality of accommodation, meals and other optional expenditures
- expense budgets based on the expected activity and quality standards for other expenditures
- specific penalties for over-claiming travel expenses, which are applied consistently and equitably
- pre-planned, authorised travel itineraries, which may be partly pre-paid, and which become the basis for advances and later claims
- where appropriate, daily rates, which are applied whatever accommodation or meal expenses are incurred
- processing all expenditure through a Staff Travel Debtors account, with offset transactions from approved travel acquittal forms
- prompt acquittal of travel expense advances and claims, particularly for interstate and overseas travel
- full reporting of all expenditure incurred by each staff member, including pre-paid, cash, account charges and credit card charges
- authorisation of actual expenditures by a person senior to the traveller.

**12.3.8 Levy-based income**

There are various levies at the state and local levels of government, such as agricultural or mineral production levies.

Controls should include

- simplifying the levy system as much as possible
- using a base that removes the incentive for the payer to distort the amount due
- ensuring that the levy relates to verifiable data
- specifying penalties for corrupt returns.

**12.3.9 Licensing and registration**

Government agencies issue or grant a variety of licences and registrations. An applicant who is not entitled to a licence might have great incentive to obtain one. The entitlement could be the means of earning income or using a substantial investment. The extra cost of an entitlement obtained through corrupt means is small in relation to the income to be gained.

A licence or registration is often granted based on the judgment of an assessor, who might be working alone. The chances for bribery are high because the risk of detection is low.

Controls can take the form of

- defining clearly the qualification rules and explaining the risks to staff
- selecting, training and counselling staff to be effective and responsible
- specifying criteria and ensuring that supporting data is verified
- careful design of licence and registration application forms to ensure all required data will be provided
- careful design of all qualifying tests, based on objective criteria
- adequate supervision and monitoring systems, to ensure that the prevention controls are effective and are being followed (while this might appear to be a *detection* control, its existence will prevent some corrupt practices).

### 12.3.10 Benefits and grants

Social security, health and employment are the major national benefit programs but there is also a range of state based benefits. These programs are also exposed to corruption if they rely only on data supplied by clients.

Controls should include

- stating the entitlement rules and evaluation criteria to all clients and staff
- training staff to properly assess applications
- designing application forms to ensure required data are provided
- basing support data on verifiable sources
- specifying penalties for corrupt claims.

### 12.3.11 Management information systems

Computer security is an area that requires sound general controls to prevent and detect corruption. Computer security seeks to prevent fraudulent use and accidental corruption of data, to maintain physical safety and the effective operation of equipment.

Computing resources and operations at risk must be identified, and the seriousness of particular risks and the value of the controls must be assessed.

Computer based risks include

- theft
- breach of copyright
- misuse of resources
- malicious damage by virus infection
- unauthorised or illegal access to a network
- unauthorised release of information.

### 12.3.12 System resources and prevention controls

- **The Data Centre** can be protected by restricting physical and remote access and by upgrading security and using more sophisticated checks and controls.
- **Remote terminals and communications** need to be secure from unauthorised access. Log-ons, security codes and passwords provide some protection but often provide a challenge to "hackers". Access logs and audit trails can identify terminals in use for particular transactions.
- **Systems software and application programs** can be protected from unauthorised modification by restricting access to program source code and computer operations. Disciplined control of program changes helps to prevent and detect unauthorised changes.
- **Data accuracy, completeness and authorisation** are the responsibilities of user departments. Control over the clerical accuracy of data includes the comparison of computer output and input totals. Exception and audit reports can identify special transactions. Data validation rules ensure that transaction records satisfy expected format and content norms.
- For **computing personnel** the levels of access and clear audit trails need to be established when dealing with network computers. Staff under undue stress need supportive counselling.

There must be a balance between the need for EDP controls and system controls that do not impede normal functions. Segregating conflicting duties is important. Segregation avoids having only one person modifying programs, accessing the tape library, preparing data and operating the computer.

Application controls ensure that programs run as expected and that data are kept secure. Data integrity ensures complete, accurate, timely and authorised records and processing.

## 13. WHAT HAPPENS WHEN CORRUPTION IS DETECTED?

Corruption can be detected at any level in an organisation. When corruption is first suspected, it is difficult to know its full extent. Suspects should not be confronted because this might alert unknown people who are colluding with the suspect. Reporting the incident to the suspect's immediate manager could alert the suspect if the manager is also corrupt. It is better to advise a senior manager outside the unit or area where the activity is taking place.

The principal officer of the organisation should establish an internal process for reporting corruption. This should specify the person(s) required to act on the information. The designated person must have senior responsibilities, possess absolute integrity and be able to operate independently. The internal auditor, a manager, or a legal officer might be suitable but the person must be of sufficient seniority to have immediate access to the principal officer.

### 13.1 Reporting to the CJC

All matters that may involve corruption should be reported to us. Absolute proof is not necessary. Reporting such matters to us is not a breach of a staff member's duty to maintain confidentiality or to abide by other policies of his or her organisation. Those who report suspected misconduct are protected by law from prosecution for breaching restrictions.

Anyone who is concerned about being victimised for reporting to us should let us know. We have the power to protect them. Those who threaten a person for reporting to us are guilty of a criminal offence and can be prosecuted. We can also seek an injunction from the Supreme Court against anyone victimising a whistleblower.

If you are uncertain whether conduct is corrupt you can contact us and seek advice.

A report should include the following details where possible:

- the name and address of the person you suspect of official misconduct

- full details of the events, dates and places concerning the suspected corrupt conduct
- the names and addresses of others who may have witnessed or have information on the corrupt conduct.

Complaints may be made in writing or verbally. Staff may refer complaints to their principal officer, their organisation's nominated Liaison Officer, or directly to our Complaints Section at:

Criminal Justice Commission  
557 Coronation Drive  
TOOWONG QLD 4066

PO Box 137  
Albert Street  
BRISBANE QLD 4002

Telephone: (07) 360 6060  
008 061 611 (Toll Free)

Facsimile: (07) 360 6333

These telephones are staffed on a 24 hour basis.

Principal officers are obliged under the *Criminal Justice Act* to refer all cases of suspected official misconduct to us as soon as they are received. We treat all matters in the strictest confidence.

### 13.2 CJC investigations

All complaints and information about suspected official misconduct, even those made anonymously, that we receive are initially handled by our Complaints Section. The person who makes the complaint will generally be interviewed by a complaints officer in person or by telephone.

Anonymous complaints are, of course, more difficult to investigate successfully without full details.

Frivolous or vexatious complaints are rejected. Persons who make false complaints that are motivated solely by malice may be prosecuted.

All genuine complaints are first assessed to determine to what degree they should be investigated. This preliminary assessment takes into account

- how long ago the alleged misconduct occurred
- the seriousness of the conduct
- the likelihood of a successful investigation
- the extent to which the complaint involves questions of public interest.

Some investigations are carried out by investigators or police officers attached to the CJC. Others are carried out by the public sector units under our supervision.

Complaints requiring detailed investigation are referred to teams in the Complaints Section or, in the case of complex or prolonged investigations, to four larger Multi-disciplinary Teams that combine the skills of investigators with those of lawyers, financial analysts, intelligence analysts, proceeds of crime specialists and surveillance and technical support personnel.

After completing these investigations, whenever practicable, we respond to those who have complained to us. If we decide to take no further action, we tell them why. If we have taken action, we tell them

- what action we have taken
- why the action was appropriate, given the circumstances of the case
- the result of the action, if we know it at the time we respond.

An investigation may result in

- a criminal charge
- disciplinary action
- a recommendation that there be administrative changes
- a recommendation that corruption prevention strategies be developed
- the complaint being dismissed as unsubstantiated.

Where appropriate we refer matters to the Director of Prosecutions or another prosecuting authority to determine whether criminal charges are warranted; or to a Misconduct Tribunal or to the appropriate public sector body for disciplinary action.

### **13.3 CJC contact with you**

We may contact you when carrying out our responsibilities to investigate and prevent corrupt conduct. If you have made a complaint we will contact you if we need further information.

We may also contact you as a result of a complaint made by someone else. We may ask you to produce a statement or specific documentation or to attend a hearing.

By contacting you we are not suggesting that you are guilty of anything. You are entitled to seek legal advice before speaking to us. We do our best to maintain discretion and confidentiality

- so that efforts to obtain the truth are not jeopardised
- to protect the reputations of people where complaints are found to be without substance
- to protect the identity of those who provide the information.

For the same reasons, you should not tell your colleagues or anyone else about your contact with us.

### **13.4 Management systems review**

After an investigation, we may decide to review the management systems of a particular public sector unit to identify any deficiencies in its operating systems and controls.

Our Corruption Prevention Division conducts these audits to help public sector units proactively reduce or avoid corruption. These audits aim to

- optimise an organisation's administrative performance, controls and accountability
- advise and assist public sector units to develop effective corruption prevention strategies

- assist in policy development and training to enhance corruption prevention practices.

We advise principal officers about four weeks before the audit begins.

Before a final report is written, we openly discuss our draft recommendations with staff who would be responsible for implementing them. These recommendations cover mechanisms and responsibilities for the implementation of improvements. Our corruption prevention officers continue to liaise closely with the client organisation during the implementation phase.

Follow up audits are conducted where our initial investigations indicate there is scope for improved management practices, improved controls and procedures and possible applicability to other areas of the organisation.



## BIBLIOGRAPHY

- Attorney General's Department 1989. *A Delicate Balance. The Place of Individual's Rights in Corruption Investigations*. The fourth International Anti Corruption Conference Papers. Canberra: AGPS.
- Australian Accounting Research Foundation Auditing Standards Board 1983. 'Statement of Auditing Practice' in *Study and Evaluation of the Accounting System and Related Internal Controls in Connection with an Audit*. (Issued 1/83).
- Australian Accounting Research Foundation Auditing Standards Board 1983. 'Statement of Auditing Practice' in *Fraud and Error*. (Issued 6/83).
- Baker and Westin 1987. 'Employee Perceptions of Workplace Crime'. US Department of Justice Bureau of Justice Statistics, May 1987.
- Bologna, G. Jack & Lindquist, Robert 1987. *Fraud Auditing and Forensic Accounting*. Toronto: Wiley.
- Challinger, Dennis 1988. 'Fraud in Government – a Criminological Overview'. *Canberra Bulletin of Public Administration*, No 56.
- Cooke, Robert Allan 1991. 'Danger Signs of Unethical Behaviour'. *Journal of Business Ethics*, Vol. 10, No 4.
- Criminal Justice Commission 1992. 'Corruption Prevention and Risk Assessment', papers from the CJC Corruption Prevention Conference held in Brisbane, May 1992.
- Department of Defence. *The Department of Defence Ethics and Fraud Awareness Campaign Discussion Kit (DEFAC)*. Canberra: Inspector General, Department of Defence.
- Dinnie, Garry 1988. 'Minimising Fraud Through Preventive Systems – Lessons from the Corporate Sector'. *Canberra Bulletin of Public Administration*, No 56.
- Electoral and Administrative Review Commission 1992. *Report on the Review of Codes of Conduct for Public Officials*. Brisbane: EARC.
- Eysenk, H 1983. *Personality Theory, Moral Development and Criminal Behaviour*. Lexington, Mass: Lexington Books.
- Fitzgerald, J & Fitzgerald A F. 1990. *Designing Controls into Computerised Systems*. Jerry Fitzgerald & Associates. Redwood City, California.
- Government of Australia 1987. *Review of Systems for Dealing with Fraud Against the Commonwealth*, a White Paper. Canberra: AGPS.
- Hefter, R 1986. 'Employee Theft: The Crippling Crime'. *Security World*, March 1986.
- Leithhead, Barry S *in press*. *Business Risk Management and Control*. Melbourne: Longman Cheshire.
- Lydon, K 1986. 'The Tempted Workforce'. *Security World*, March 1986.
- Madsen, P and Shafritz, J M (eds) 1992. *Essentials of Government Ethics*. Harmondsworth: Penguin Books.
- Mair, W C, et al. 1978. *Computer Control & Audit*. Altamonte Springs, Florida: Institute of Internal Auditors.
- Nettler, Gwynn 1982. *Lying Cheating and Stealing*. Cincinnati: Anderson Publishing.

- Parliamentary Criminal Justice Commission 1991. *Report No. 13*. Brisbane: CJC.
- Public Sector Management Standard for Performance Planning and Review 1985. Brisbane: Public Sector Management Commission.
- Public Sector Management Standard for Recruitment and Selection 1991. Brisbane: Public Sector Management Commission.
- Public Sector Management Standard for Position Descriptions 1992. Brisbane: Public Sector Management Commission.
- Public Sector Management Standard for Grievance Procedures 1991. Brisbane: Public Sector Management Commission.
- Public Sector Management Standard for Executive Performance Management and Development 1991. Brisbane: Public Sector Management Commission.
- Public Sector Management Standard for Fair Treatment of Employees 1992. Brisbane: Public Sector Management Commission.
- Queensland Public Sector Finance and Management Standards 1991. Brisbane: Goprint
- Queensland Treasury 1990. *Public Finance Standards with explanatory overview*. Brisbane: Goprint (with subsequent amendments in 1991)
- Richter, W L, et al. 1990. *Combating Corruption: Encouraging Ethics*. Washington, D C: American Society for Public Administration.
- Royal Australian Institute of Public Administration 1990. *Do Unto Others*. Proceedings and Papers of a Conference held in Brisbane, November 1990.
- Royal Australian Institute of Public Administration and the Australian Institute of Criminology 1988. 'Fraud in the Public Sector', proceedings of two conferences in *Canberra Bulletin of Public Administration*.
- Shepard, Ira & Duston, Robert 1988. *Thieves at Work*. Washington: Bureau of National Affairs.
- The Institute of Internal Auditors 1985. *Deterrence, Detection, Investigation, and Reporting of Fraud*. Statement on Internal Auditing Standards No. 3, May 1985. Altamonte Springs, Florida.
- The Institute of Internal Auditors 1983. *Control: Concepts and Responsibilities*. Statement on Internal Auditing Standards No. 1, July 1983. Altamonte Springs, Florida.
- Thiroux, J P 1990. *Ethics: Theory and Practice*. 4th edition. New York: Macmillan 1990
- Thompson, Courtenay 1990. 'Red Flags', a paper given at The Institute of Internal Auditors International Conference in St Louis, Missouri, June 1990.
- Yochelson, S & Samenow, S 1976. *The Criminal Personality*. New York: Aronson.

## APPENDIX 1 - ADDITIONAL RESOURCES

### Auditing Standards

Two useful items of reference are:

1. *Internal Auditing Standards No. 1 – Control: Concepts and Responsibilities* (July 1983)  
  
This statement provides guidance to internal auditors on the nature of control and the roles of the participants in its establishment, maintenance, and evaluation.
2. *Internal Auditing Standards No. 3 – Deterrence, Detection, Investigation, and Reporting of Fraud* (May 1985)  
  
This statement interprets the Standards and establishes guidelines for internal auditors regarding their responsibility for deterring, detecting, investigating, and reporting of fraud. It does not provide guidance on specific audit procedures used in performing audits; rather, it establishes guidelines by which internal auditors conform their activities with the stated concepts of due professional care.

### RISK ASSESSMENT

#### Software

There is a limited range of specialised PC software suitable for corruption risk analysis, including:

1. Risk Assessment Toolkit, available from:  
  
The Institute of Internal Auditors Inc.  
249 Maitland Avenue  
Altamonte Springs, Florida 32701-4201  
  
Facsimile Number: 0015 1 407 831 5171  
  
Cost: Approx. \$US100, plus air freight. (credit card)  
  
The package is primarily designed for internal audit planning, to assess the risks of auditable units and determine a priority for audit attention. The approach can be used just as well to assess the corruption risk, rather than the total business risk.  
  
The Toolkit contains a brief text description of internal audit planning and a diskette of Lotus 1-2-3 templates.

2. RANK-IT is a risk ranking program available from:

Jerry FitzGerald & Associates  
506 Barkentine Lane,  
Redwood City, California 94065

Facsimile Number: 0015 1 415 593 9316

Cost: Approx. \$US100, plus air freight.

RANK-IT can be used to rank any kind of risk. The package produces a ranking worksheet, accepts scores from the assessor or Delphi group, calculates the ranking and produces a ranked list. RANK-IT comprises a 40-page manual and a software diskette. Simple to use. A demo diskette is available from:

InCheck Systems  
PO Box 714  
Liverpool 2170

Telephone Number: (02) 774 5914

3. The Fraud Detection Matrix is available from:

Clintons Financial Services  
1529 Notre Dame Drive,  
Davis, California 95616

Cost: \$US295 plus air freight

The Fraud Detection Matrix (FDM) provides three types of business entities and eighteen types of business activities. Simple fraud exposures, symptoms and audit steps have been set for each activity.

The program allows the user to add entries, activities, exposures, symptoms and audit steps. The program provides a framework, rather than extensive detail, to guide the user. A demo diskette is available from InCheck Systems.

4. A Fraud Risk Questionnaire and Assessment Model (RQUEST) is available from InCheck Systems. The package was developed for use in an Australian Government department and comprises a text template for the 120-question survey, response-summarising spreadsheet templates and a complex calculation model on Lotus 1-2-3.

Cost: Approx. \$350.

5. CONTROL-IT is a risk-control evaluation package available from Jerry FitzGerald & Associates. The package is built around three databases of risks, business elements at risk and controls. The package prepares a matrix of items drawn from the databases.

CONTROL-IT was designed for *Designing Controls into Computerised Systems*, the title of FitzGerald's book on the subject. While the databases contain entries for computerised systems, the package can be used for any risk-analysis application. The user can add to or delete records from the databases as required.

The package comes with an extensive manual and part of the disk set is a training program in the methodology. CONTROL-IT is not easy to use. A demo diskette is available from InCheck Systems.

FitzGerald's book is a useful companion to the software and offers many controls for computerised systems. His six-point audit process is very clearly described.

Cost: CONTROL-IT approx. \$US700 plus air freight

The book is approximately \$US20

The software described in this section has been collected through the consulting activities of Leithhead & Associates, who assisted us in compiling this manual.

InCheck Systems is an independent consultancy, specialising in personal computer systems, internal auditing and training. Its principal consultant is Neil E Maddock, B Comm, AASCPA, Grad Dip Ed(Tech).

## RESOURCES ON ETHICS

There are several professional ethics programs which can advise public-sector managers on how to develop an understanding of ethics in their corruption-prevention programs.

- In the Brisbane area, the Queensland University of Technology, Griffith University and Bond University have ethics programs.
- The Queensland University of Technology Unit for Applied Ethics and Human Change have developed a Public Sector Ethics Initiative.

Contact: QUT Unit for Applied Ethics and Human Change  
Faculty of Arts  
Carseldine Campus  
PO BOX 284  
Zillmere Q 4034

Resources and advice in public sector ethics can be obtained from sources such as the following:

The Integrity in Government Project  
c/- Dr P. Finn and Dr J. Uhr  
Australian National University  
GPO Box 4  
Canberra 2601

Government Ethics Centre  
Josephson Institute of Ethics  
310 Washington Blvd  
Suite 104  
Marina del Rey, CA 90292

Dr John Langford  
c/- Department of Public Administration  
University of Victoria  
Victoria, BC, Canada

## APPENDIX 2 - QUEENSLAND PUBLIC FINANCE STANDARDS (extract)

### Selected References to Internal Control

#### 210 Revenue identification and control

2. The necessary procedures shall be established and specified in the accounting manual with the objective of ensuring:
  - (a) prompt recognition and recording of revenue in the accounts in a manner which allows reporting objectives and accountability requirements to be satisfied;
  - (b) operational responsibility, subject to defined policy, is assigned for the management of revenue and of identifying revenue however occurring or accruing;
  - (c) control over the prompt and correct assessment of revenue claimable;
  - (d) revenue is safeguarded from loss and is not foregone, waived, remitted or written off except where authorised by a competent authority or duly authorised person;
  - (e) gains qualifying for recognition as revenue are promptly brought to account;
  - (f) that accounting policies to be applied in the recognition of revenue in the accounts and/or as general disclosures in notes to the financial statements are defined and consistently applied.

#### 220 Expense Identification and Control

2. The necessary procedures shall be established and specified in the accounting manual with the objective of ensuring:
  - (a) prompt recognition and recording of expense in a manner which allows reporting objectives and accountability requirements to be satisfied;
  - (b) systems of approval and control are in place and are adequate to ensure

expense is only incurred for an authorised (official) purpose which shall be recorded and kept;

- (c) competitive procurement arrangements are in place including, where applicable, those required by the State Purchasing Policy approved by State Cabinet;
- (d) operational responsibility is assigned for the management of expense in terms of strategic plans and of identifying expense otherwise occurring or accruing;
- (e) that the accounting policies to be applied in the recognition of expense in the accounts and/or as general disclosures in notes to the financial statements are defined and consistently applied.

#### 230 Asset Identification and Control

2. The necessary procedures shall be established and specified in the accounting manual with the objective of ensuring:
  - (a) proper application of the prescribed requirements and of policy determined by State Cabinet, the appropriate Minister or other competent authority, in regard to the acquisition, holding and disposal of assets;
  - (b) the acquisition or receipt of assets and the disposal, issue or disbursement of assets is authorised and performed by a competent authority or duly authorised persons in accordance with the prescribed requirements, including in regard to the receipt and payment of cash, to the extent practicable, the Practice Statements given in Part 2 Division 3 of Schedule A of these Public Finance Standards;
  - (c) efficiency and economy in the acquisition, use and disposal of assets;
  - (d) prompt recognition and recording in the accounts of particulars, including the cost and such other values, of assets and transactions in regard thereto, in a manner which allows reporting and accountability requirements to be satisfied;
  - (e) adequate protection of assets;

- (f) transactions are supported by readily accessible records and documentation;
- (g) the existence of assets is verified no less frequently than annually and a reconciliation of relevant balances is performed at appropriate times having regard to the propensity for errors or loss;
- (h) consistent methods are applied by persons responsible for the recognition of and accounting for assets;
- (i) that where circumstances permit, duties of approving, accounting and custody are segregated to provide effective internal control;
- (j) goods, services or works are not provided by a department or statutory body on credit except
  - (i) for approved classes of business;
  - (ii) where the client eligibility criteria and applicable terms are defined;
  - (iii) to the extent relevant, the Practice Statement - Receivables given in Part 2 Division 3 of Schedule A to these Public Finance Standards is instituted.

#### **234 Loss and Accumulated Depreciation of Assets**

1. For the purposes of this Public Finance Standard:

'losses' has the meaning given in the Act and is extended to cover money and property of a statutory body.

Deficiencies and shortages detected in money and property shall be the subject of an immediate internal report. Where the report indicates the loss may have arisen from a cause that could constitute an offence under The Criminal Code or any other Act or law, notice in writing shall be given to a member of the Police Force of the jurisdiction appropriate to the circumstances and to the Auditor-General or where the Auditor-General is exempted from such audit such other auditor appointed pursuant to section 59 of the Act and, where appropriate, Criminal Justice Commission.

240

#### **Liability Identification and Control**

2. The necessary procedures shall be established and specified in the accounting manual with the objective of ensuring:
  - (a) for the employment of persons, is in accordance with the requirements of applicable Acts, industrial awards and the like;
  - (b) for the procurement of goods and services, whether through Government agencies, the letting of contracts or otherwise, is, where applicable, in accordance with the State Purchasing Policy approved by State Cabinet;
  - (c) for borrowing or financial arrangements has the approvals as may be required under the Statutory Bodies Financial Arrangements Act and any other Act or law and, in the case of financial arrangements under the Statutory Bodies Financial Arrangements Act, has the sanction of the Treasurer before any negotiation is commenced;
  - (d) can be satisfied when due for payment either from identified funds available under an approved budget or from programmed funds under an approved forward plan or arrangement;
  - (e) is necessary and for identified official purposes and is firstly approved by a competent authority or person delegated in writing to so approve;
  - (f) subject to over-riding legal considerations, is in the name of the department or statutory body;
  - (g) is supported by readily accessible records and documentation systematically filed and securely stored.
3. Procedures shall be established and specified in the accounting manual setting forth the methods to be consistently applied and the positions or persons responsible for accounting for all liabilities which the department or statutory body will be required to settle, including:
  - (a) current liabilities, including:-
    - (i) accounts payable;

- (ii) end of year accounting adjustments on account of material accruing items;
  - (iii) unearned revenue where there is an obligation to provide future benefits or in default to refund;
  - (iv) other items where settlement during the next twelve months in probable employee entitlements including any accrued annual leave, long service leave, any superannuation obligation the department or statutory body is responsible for and in the case of sick leave.
- (b) (i) all of the current entitlements where accrued and payable on termination of services; or
  - (ii) where not so payable, that part of the entitlement accrued that will be required to satisfy any eligible claim arising from a past event;
- (c) claims incurred but not reported under superannuation, insurance, grant or subsidy schemes;
  - (d) borrowings, debts servicing and other financial arrangements;
  - (e) distributable amounts;
  - (f) other material liabilities.

## 250 Equity Identification and Control

- 2. Adequate systems shall be established and maintained, by an accountable officer and by a statutory body, to monitor and ensure that subject to paragraph (1) of this Public Finance Standard, the equity (net assets)
  - (a) is identified and recorded
  - (b) as the case requires, is maintained in accordance with —
    - (i) the requirements of any Act or law
    - (ii) any approved strategic plans or economic (financial) objectives, and shall include adequate internal controls (including as appropriate those set forth in Public Finance Standard 622).

- 3. Any necessary procedures associated with the system referred to in paragraph (2) shall be established and specified in the accounting manual with the objective, as the case requires, of ensuring:

- (a) persons or entities can be identified with subscribed amounts that in terms of requirements under any Act or in terms of a recognised Statement of Accounting Concepts or Australian Accounting Standard qualify for recording as equity;
- (b) separate recording of amounts appropriate from profits/surpluses or from reserves;
- (c) grants (where qualifying to be recorded as equity) as supported by records setting forth relevant particulars including whether associated assets are for the unrestricted use or whether restrictions on use apply;
- (d) asset revaluation and other authorised reserves are properly established and kept;
- (e) appropriations for distribution to equity interests are approved by a competent authority and properly recorded in the accounts.

## 310 Program Management

- 2. The following elements shall, as a minimum, be included in the program management system within the department or statutory body:

- (a) a strategic plan which shall:
  - (i) set forth the desired position over the next five year (or longer) period
  - (ii) be determined following an analysis of all relevant environmental factors
  - (iii) provide a focus for annual budgetary and resource management strategies and decisions;

- (b) a system of resource management which shall focus on the outputs and outcomes achieved by its programs. Such a system shall:
  - (i) include a clear linkage with the strategic plan
  - (ii) group activities according to common purposes (programs) for the purpose of management decisions and resource allocation and
  - (iii) include clearly stated, measurable objectives for each program
- (c) a systematic performance evaluation and review, including of program effectiveness and efficiency which shall determine as a minimum whether:
  - (i) the policies, goals (as embodied in the Strategic Plan) and program objectives remain appropriate and are being achieved
  - (ii) resources are optimally allocated across programs
  - (iii) resources are optimally utilised within each program.

## 622 Internal Control

1. Adequate systems of internal control and reporting shall be established and maintained to assist the accountable officer of each department and each statutory body to monitor and ensure:

- (a) the prescribed requirements
  - (i) under section 36(1) of the Act in the case of an accountable officer
  - (ii) under section 46C of the Act in the case of a statutory body and
  - (iii) in either case under these Public Finance Standards, are complied with;
- (b) operational practice and procedure is formally approved by the accountable officer or statutory body and suitably set forth in the accounting manual including
  - (i) the locations which shall be identified on all relevant stationery to indicate the principal place of business and places for the receipt of monies, goods etc. and for the lodgment of claims and the like
  - (ii) the persons responsible for the security, custody and as the case requires prompt acknowledgment of revenue and assets accepted by the department or statutory body
  - (iii) the arrangements that apply in ensuring the approval of expenses, acquisition of assets or the incurrence of liabilities are for authorised (official) purposes only and that the approval and procedure for the disposition of any asset is in accordance with the prescribed requirements
  - (iv) the persons responsible for verifying the existence and condition of assets in each financial year and, subject to these public finance standards, the frequency of such verifications having regard to risk, materiality, staff changes and the like
  - (v) where staff resources permit, arrangements for segregation of duties to enhance internal check and control consistent with risks involved;
- (c) adequate organisational and accounting practice and procedure is established to ensure accounts and accounting records, whether computer based or otherwise, are
  - (i) subject to adequate and effective checks and balances to preserve the integrity and accuracy thereof and to ensure the reliability of financial reports
  - (ii) kept secure and protected from unauthorised access or alteration
  - (iii) printed, typed or written in permanent ink where kept as hard copy and that any errors corrected are initialled and dated



- (iv) retained in accordance with Public Finance Standard 401.
- 2. Where computerised accounting systems are employed by an accountable officer or by a statutory body, either for internal use or as an agency for another department or statutory body those systems shall be:
  - (a) thoroughly tested and proven before becoming operational and any master files created shall be checked to ensure they are correct
  - (b) subject to adequate management and organisational controls
    - (i) over the functions related to processing
    - (ii) to ensure the systems are developed or modified in accordance with management approved plans and procedures
    - (iii) to ensure that procedures are established which will reduce the likelihood of failures and, where failures do occur, enable complete and timely recovery.
- 3. Where an accountable officer or a statutory body has information processed by the Centre for Information, Technology and Communications or another external agency, adequate arrangements shall be agreed and established to ensure:
  - (a) that where an agency other than the Centre for Information, Technology and Communications is used that security, confidentiality, processing priorities and data back-up systems are adequate;
  - (b) that all documents submitted for processing are accounted for on reports received from the agency;
  - (c) that where the value of items submitted for processing can be reconciled with processing results such reconciliations are promptly performed or, where not practicable, that audit trails are such that any sample of individual items submitted for processing can be identified on output reports and the correctness of computations and accumulations verified.

- (4) The use of impressed or lithograph signatures on accounting records is prohibited, except where authorised by the appropriate accountable officer or statutory body and used in connection with the issue of cheques, group certificates and like output documents where legally acceptable and in accordance with control procedures set forth in the accounting manual.

## 624 Credit Card Organisations

- 1. Where an accountable officer or a statutory body is of the opinion that it is cost effective to accept payment of amounts owing, other than taxation payable to the Consolidated Revenue Fund, through a credit card organisation he may enter into arrangements and introduce procedures which shall be specified in the accounting manual to ensure that the accounting officer accepting payment from a person or entity using a credit card facility is aware of all obligations including:
  - (a) obtaining authorisation for sales in excess of an Authorised Floor Limit;
  - (b) detecting unauthorised or forged signatures;
  - (c) ensuring an expired credit card facility is not accepted; and
  - (d) not processing transactions where a credit card tendered is listed on a Warning Bulletin.
- 2. An accountable officer or statutory body may enter into an arrangement for credit card facilities to be made available provided that:
  - (a) the use of an official credit card facility is generally restricted to senior officers required to travel or entertain on a frequent basis or is restricted to specific purchases such as with 'fuel cards', 'toll cards' and the like;
  - (b) where practicable, only one account shall be opened with the credit organisation, which account shall be in the name of the department or statutory body;
  - (c) only authorised charges may be made by the credit organisation
  - (d) the arrangements entered into either:

- (i) allow individual card limits to be applied and provide security against unauthorised use; or
  - (ii) do not involve the department or statutory body in any liability for unauthorised use of individual cards by the user or otherwise;
- (e) the credit organisation furnishes the department with a monthly statement or record of transactions and balances;
- (f) the arrangements in place ensure the credit cards are used for official purposes only and that any misuse is promptly detected through the operation of internal control measures and reported to the accountable officer or the chairman of the statutory body;
- (g) the person using credit cards obtains or otherwise maintains particulars of each use of the credit card including supporting invoices and dockets etc, which shall be attached to the credit card transaction record for the purposes of substantiating the official use of the card and settlement of the account within the settlement period.
4. A member, officer or employee of a department or statutory body may accept a benefit, not being a benefit referred to in paragraph (3) hereof, provided that:
- (a) in the case of normal entertainment, hospitality and minor presentations of no significance or lasting real value which conform with industry/country norms, the circumstances and the benefit involved are advised to his senior officer as specified in the accounting manual;
  - (b) in all other cases, a reportable gift declaration shall be made in the form and in accordance with procedures set forth in the accounting manual in order that the matter may be formally recorded in accordance with this Public Finance Standard.
- Provided that this Public Finance Standard shall not be construed to prohibit the pursuit of financial assistance or donations to a department or statutory body where such pursuit is in accordance with the Collections Act or is otherwise authorised in law.
- For the purposes of this Public Finance Standard:-

#### 625 Conflicts of Interest

1. Each accountable officer of a department and each statutory body shall specify in the accounting manual and disseminate by way of an approved code of conduct or otherwise, principles and procedures to safeguard members, officers or employees thereof from being involved in a situation which could lead to or be seen to give rise to a conflict of interest.
  3. A member, officer or employee of a department or statutory body shall not:
    - (a) solicit any benefit from persons other than his employer in connection with his official functions and duties;
    - (b) accept any benefit other than from his employer for any official function or duties performed or not performed which could create a conflict of interest or be seen to create such conflict;
    - (c) accept any gift of money or benefit by way of loans and the like for any functions or duties performed or not performed.
- 'reportable gift' means any gift of property, travel, entertainment, hospitality or any other benefit which is not consistent with industry/country norms. The term includes in any case valuable items of property whether of a personal nature or otherwise (for example, ornate or precision display items such as clocks, furniture, figurines, works of art and the like and other items of enduring value including jewellery and personal items containing precious metals or stone or fine art work).

## **APPENDIX 3 - STATEMENT OF AUDITING PRACTICE AUP 12**

(Issued 1/83)

Australian Accounting Research Foundation

Auditing Standards Board

### **Statement of Auditing Practice**

#### **Study and Evaluation of the Accounting System and Related Internal Controls in Connection with an Audit**

##### **Introduction**

1. Statement of Auditing Standards AUS 1(para. 22) states:

"22. The Auditor should gain an understanding of the accounting system and related internal controls and should study and evaluate the operation of those internal controls upon which he wishes to rely in determining the nature, timing and extent of other audit procedures."

The purpose of this Statement is to provide guidance as to procedures to be followed to comply with this basic principle in connection with the audit of financial information. In this Statement, the term "financial information" encompasses financial statements.

##### **Accounting System and Internal Control**

2. Management is responsible for maintaining an adequate accounting system incorporating various internal controls to the extent appropriate to the size and nature of the business. The auditor needs reasonable assurance that the accounting system is adequate and that all the accounting information which should be recorded has in fact been recorded. Internal controls normally contribute to such assurance.
3. An accounting system can be defined as the series of tasks in an entity by which transactions are processed as a means of maintaining financial records. Such a system should recognize, calculate, classify, post, summarize and report transactions.

4. The system of internal control is the plan or organization and all the methods and procedures adopted by the management of an entity to assist in achieving management's objective of ensuring, as far as practicable, the orderly and efficient conduct of its business, including adherence to management policies, the safeguarding of assets, the prevention and detection of fraud and error, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information. The system of internal control extends beyond those matters which relate directly to the functions of the accounting system. The individual elements of the system of internal control are referred to as internal controls and are collectively known as internal control.

5. An accounting system supplemented by effective internal controls can provide management with reasonable assurance that assets are safeguarded from unauthorized use or disposition and that financial records are reliable to permit the preparation of financial information.

6. The environment in which internal control operates has an impact on the effectiveness of the specific control procedures. A strong control environment, for example, one with tight budgetary controls and effective internal audit function, can significantly complement specific control procedures. However, a strong environment does not, by itself, ensure the effectiveness of the overall system of internal control. The internal control environment may be affected by:

##### **(a) Organizational structure**

The organizational structure of an entity serves as a framework for the direction and control of its activities. An effective structure provides for the communication of the delegation of authority and the scope of responsibilities. It should be designed, insofar as practicable, to preclude an individual from overriding the control system and should provide for the segregation of incompatible functions. Functions are incompatible if their combination may permit the commitment and concealment of fraud or error. Functions that typically are segregated are access to assets, authorization, execution of transactions, and record-keeping.

## (b) Management supervision

Management is responsible for devising and maintaining the system of internal control. In carrying out its supervisory responsibility, management should review the adequacy of internal control on a regular basis to ensure that all significant controls are operating effectively. When an entity has an internal audit department, management may delegate to it some of its supervisory functions, especially with respect to the review of internal control. This particular internal audit function constitutes a separate component of internal control undertaken by specially assigned staff within the entity with the objective of determining whether other internal controls are well designed and properly operated.

## (c) Personnel

The proper functioning of any system depends on the competence and honesty of those operating it. The qualifications, selection and training as well as the personal characteristics of the personnel involved are important features in establishing and maintaining a system of internal control.

**Objectives of Internal Control**

7. Internal controls relating to the accounting system are concerned with achieving the following objectives:
- (a) transactions are executed in accordance with management's general or specific authorization;
  - (b) all transactions are promptly recorded in the correct amount, in the appropriate accounts and in the accounting period in which executed so as to permit preparation of financial information within a framework of recognized accounting policies and to maintain accountability for assets;
  - (c) access to assets is permitted only in accordance with management's authorization; and
  - (d) The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with regard to any differences.

8. Specific internal control procedures designed to achieve such objectives could include checking the arithmetical accuracy of the records; the maintenance of reconciliations, edit routines, control accounts and trial balances; approval and control of documents; comparison with external sources of information; comparing the results of cash, security and inventory counts with accounting records; limiting direct physical access to assets and records; and comparison of results with budget.

**Inherent Limitations of Internal Control**

9. Internal control can provide only reasonable assurance that management's objectives are reached because of inherent limitations of internal control, such as:
- (a) management's usual requirement that a control be cost-effective, i.e., that the cost of a control procedure not be disproportionate to the potential loss due to fraud or error;
  - (b) the fact that most controls tend to be directed at anticipated types of transactions and not at unusual transactions;
  - (c) the potential for human error due to carelessness, distraction, mistakes of judgment or the misunderstanding of instructions;
  - (d) the possibility of circumvention of controls through collusion with parties outside the entity or with employees of the entity;
  - (e) the possibility that a person responsible for exercising control could abuse that responsibility, for example, a member of management overriding a control;
  - (f) the possibility that procedures may become inadequate due to changes in condition and compliance with procedures may deteriorate.

## Audit Procedures

10. The auditor, in forming his opinion on financial information, needs reasonable assurance that transactions are properly recorded in the accounting records and that transactions have not been omitted. Internal controls, even if fairly simple and unsophisticated, may contribute to the reasonable assurance the auditor seeks. The auditor's objective in studying and evaluating internal controls is to establish the reliance he can place thereon in determining the nature, timing and extent of his substantive auditing procedures.
11. The auditor obtains an understanding of the accounting system to identify points in the processing of transactions and handling of assets where errors or fraud may occur. When the auditor is relying on internal control, it is at these points that he must be satisfied that internal control procedures applied by the entity are effective for his purpose.
12. Compliance procedures are tests designed to obtain reasonable, but not absolute, assurance that those internal controls on which audit reliance is to be placed are in effect. These procedures include tests requiring inspection of documents supporting transactions to gain evidence that controls have operated properly (for example, verifying that the document has been authorized) and enquiries about the observation of controls which leave no audit trail (for example, determining who actually performs each function not merely who is supposed to perform it).
13. Substantive procedures are designed to obtain evidence as to the completeness, accuracy and validity of the data procedure by the accounting system. These procedures include tests of details of transactions and balances, and analyses of significant ratios and trends, including the resulting investigation of unusual fluctuations and items.
14. While compliance procedures and substantive procedures are distinguishable as to their purpose, the results of either type of procedure may contribute to the purpose of the other. Errors discovered in conducting substantive procedures may cause the auditor to modify his previous evaluation that controls were adequate for his purposes.

## Review and preliminary evaluation

15. The auditor should review significant areas of the accounting system and related internal controls to gain an understanding of the flow of transactions and the specific control procedures to be able to make a preliminary evaluation and identification of those internal controls on which it might be effective and efficient to rely in conducting his audit.
16. The review of internal control consists mainly of enquiries of personnel at various organizational levels within the entity, together with reference to documentation such as procedures manuals, job descriptions and flow charts to gain knowledge about the controls which the auditor has identified as significant to his audit. In a continuing engagement, the auditor will be aware of internal controls through work carried out previously but will need to update his knowledge.
17. It may be useful to trace a few transactions through the accounting system to assist in understanding that system and its related internal controls. When the transactions selected are representative of the type of transactions that usually pass through the system, this procedure may be treated as part of the compliance procedures.
18. The auditor should enquire about whether the internal controls were in use throughout the period of intended reliance. If substantially different controls were used at different times during the period, the auditor should consider each separately. A breakdown in internal controls for a specific portion of the period of intended reliance would necessitate separate consideration of the nature, timing and extent of the audit procedures to be applied to transactions of that period.
19. Different techniques may be used to record information relating to an internal control system. Selection of a particular technique is a matter for the auditor's judgment. Common techniques, used alone or in combination, are narrative descriptions, questionnaires and flow charts. The extent of the auditor's record of internal controls will vary depending on the reliance he intends to place on those controls.

20. The auditor's preliminary evaluation of the internal controls should be made on the assumption that the controls operate generally as described and that they function effectively throughout the period of intended reliance. The purpose of the preliminary evaluation is to identify the particular controls on which the auditor still intends to rely and to test through compliance procedures.
21. The auditor may decide not to rely on particular internal controls because, for example,
- (a) they are defective in design and therefore their operation would provide insufficient assurance as to the accuracy and completeness of information produced by the accounting system, or
  - (b) the audit effort required to test compliance with those internal controls would exceed the reduction in effort that could be achieved by reliance on them.
25. If, based on the results of his compliance procedures, the auditor concludes that it is not appropriate to rely on a particular internal control to the degree previously contemplated, he should ascertain whether there is another control which would satisfy his purpose and on which he might rely (after applying appropriate compliance procedures). Alternatively, he may modify the nature, timing or extent of his substantive audit procedures.
26. The auditor's compliance procedures normally should be applied to transactions selected from those of the whole period under examination. When, however, a shorter period is initially tested, the auditor needs to consider what is necessary to provide reasonable assurance as to the reliability of the accounting records for the whole period. The auditor's judgment as to the nature, timing and extent of compliance or substantive procedures to be applied to transactions occurring in the remaining period will be affected by such factors as the following:

#### Compliance Procedures

22. Compliance procedures should be conducted by the auditor to gain evidence that those internal controls on which he intends to rely operate generally as identified by him and that they function effectively throughout the period of intended reliance. The concept of effective operation recognizes that some deviation from compliance may have occurred.
23. Deviations from prescribed controls may be caused by such factors as changes in key personnel, significant seasonal fluctuations in volume of transactions, and human error. The auditor should make specific enquiries concerning these matters, particularly as to the timing of staff changes in key control functions. He should then ensure that his compliance procedures appropriately cover such a period of change or fluctuation.
24. Based on the results of his compliance procedures, the auditor should evaluate whether the internal controls are adequate for his purposes. The reliance which is appropriate depends on the level of the auditor's assurance as to the effective operation of the controls.
- (a) the results of the procedures already conducted;
  - (b) the responses to enquiries as to whether the internal control system is still operating in the same manner as when studied and evaluated;
  - (c) the length of the remaining period;
  - (d) the nature and amount of the transactions or balances involved;
  - (e) the auditor's evaluation of the internal control environment, especially supervisory controls; and
  - (f) the substantive procedures which the auditor intends to carry out irrespective of the adequacy of internal controls.

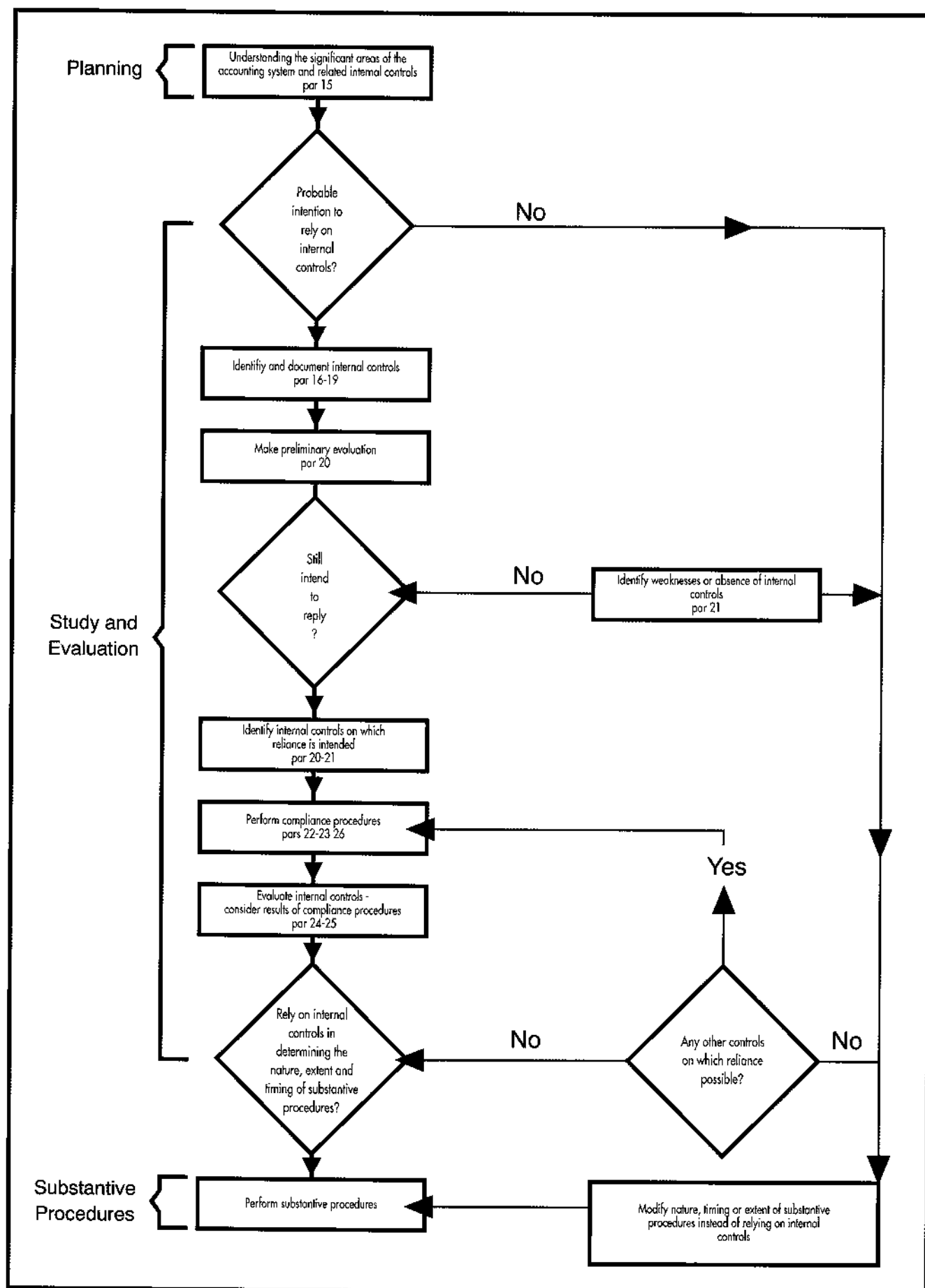
### **Internal Controls in the Small Business**

27. The auditor needs to obtain the same degree of assurance in order to give an unqualified opinion on the financial statements of both small and large entities. However, many controls which would be relevant to large entities are not practical in the small business. For example, in small businesses, accounting procedures may be performed by few persons. These persons may have both operating and custodial responsibilities, and segregation of functions may be missing or severely limited. Inadequate segregation of duties may, in some cases, be offset by owner/manager supervisory controls which may exist because of direct personal knowledge of the business and involvement in the business transactions. In circumstances where segregation of duties is limited and evidence of supervisory controls is lacking, the evidence necessary to support the auditor's opinion on the financial information may have to be obtained largely through the performance of substantive procedures.

### **Communication of Weakness in Internal Control**

28. As a result of his study and evaluation of internal control and other auditing procedures, the auditor may become aware of weakness in internal control. For the benefit of his client, the auditor should make management aware, on a timely basis, of material weaknesses which have come to his attention. Such weaknesses are usually communicated in writing. It is important to indicate in the letter that it discusses only weaknesses which have come to the attention of the auditor as a result of his audit, and that his examination has not been designed to determine the adequacy of internal controls for management purposes.
29. The flowchart below illustrates the study and evaluation of the accounting system and related internal controls.

## Study and Evaluation of the Accounting System and Related Internal Controls - An Illustration



NOTE: The above illustrates the study and evaluation of the accounting system and related internal controls.



## APPENDIX 4 - STATEMENT OF AUDITING PRACTICE AUP 16

(Issued 6/83)

Australian Accounting Research Foundation

Auditing Standards Board

### Statement of Auditing Practice

#### Fraud and Error

##### Introduction and Definitions

1. Statement of Auditing Standards, AUS 1 (para. 12) states:

"In forming his opinion on the financial information, the auditor carries out procedures designed to obtain reasonable assurance that the financial information is properly stated in all material respects. Because of the test nature and other inherent limitations of an audit, together with the inherent limitations of any system of internal control, there is an unavoidable risk that even some material misstatement may remain undiscovered. However, any indication that some fraud or error may have occurred which could result in material misstatement would cause the auditor to extend his procedures to confirm or dispel his suspicions."

In this Statement the term "financial information" encompasses financial statements.

The purpose of this Statement is to discuss the auditor's responsibility for the detection of material misstatements resulting from fraud or error when carrying out an audit of financial information and to provide guidance as to the procedures that the auditor should perform when he encounters circumstances that cause him to suspect, or when he determines, that fraud or error has occurred.

2. The term "fraud" refers to misappropriation of assets or intentional misrepresentations of financial information by one or more individuals among management, employees, or third parties. Fraud may involve:
  - (a) manipulation, falsification or alteration of records or documents;

- (b) suppression or omission of the effects of transactions from records or documents;
- (c) recording of transactions without substance; or
- (d) misapplication of accounting policies.

3. The term "error" refers to unintentional mistakes in financial information, such as:

- (a) mathematical or clerical mistakes in the underlying records and accounting data;
- (b) oversight or misinterpretation of facts; or
- (c) misapplication of accounting policies.

##### Responsibility for the Detection of Fraud and Error

4. The responsibility for the prevention and detection of fraud and error rests with management through the implementation and continued operation of an adequate system of internal control. Such a system reduces but does not eliminate the possibility of fraud or error.
5. The objective of an audit of financial information is to enable an auditor to express an opinion on such financial information. In forming his opinion, the auditor carries out procedures designed to obtain evidence that will provide reasonable assurance that the financial information is properly stated in all material respects. Consequently, the auditor seeks reasonable assurance that fraud or error which may be material to the financial information has not occurred or that, if it has occurred, the effect of fraud is properly reflected in the financial information or the error is corrected. The auditor, therefore, should plan his audit so that he has a reasonable expectation of detecting material misstatements in the financial information resulting from fraud or error. The degree of assurance of detecting errors would normally be higher than that of detecting fraud, since fraud is usually accompanied by acts specifically designed to conceal its existence.
6. Due to the inherent limitations of an audit (see paragraphs 7-10) there is a possibility that material misstatements of the financial

information resulting from fraud and, to a lesser extent, error may not be detected. The subsequent discovery of material misstatement of the financial information resulting from fraud or error existing during the period covered by the auditor's report does not, in itself, indicate that the auditor has failed to adhere to the basic principles governing an audit. The question of whether the auditor has adhered to the basic principles governing an audit is determined by the adequacy of the procedures undertaken in the circumstances and the suitability of the auditor's report based on the results of these procedures.

#### **Inherent Limitations of an Audit**

7. The test nature of an audit of financial information involves judgment as to the areas to be tested and the number of transactions to be examined. Furthermore much audit evidence is persuasive rather than conclusive in nature. Therefore, the auditor's examination is subject to the inherent risk that some material misstatements of the financial information resulting from fraud or error, if either exists, will not be detected.
8. The risk of not detecting material misstatement resulting from fraud is greater than the risk of not detecting a material misstatement resulting from error because fraud usually involves acts designed to conceal it, such as collusion, forgery, deliberate failure to record transactions, or intentional misrepresentations being made to the auditor. Unless the auditor's examination reveals evidence to the contrary, he is entitled to accept representations as truthful and records and documents as genuine. However, the auditor should plan and perform his audit with an attitude of professional scepticism recognizing that he may encounter conditions or events during his examination that would lead him to question whether fraud or error exist.
9. While the existence of an effective system of internal control reduces the probability of misstatement of financial information resulting from fraud or error, there will always be some risk of internal controls failing to operate as designed. Furthermore, any system of internal control may be ineffective against fraud committed by management. Certain levels of management may be in a position to override controls that would prevent similar frauds by other employees; for example, by directing subordinates to

record transactions incorrectly or to conceal them, or by suppressing information relating to transactions.

10. Statement of Auditing Practice AUP 9, Audit Engagement Letters, paragraph 4, recommends that engagement letters include reference to the inherent limitations of an audit and the fact that material misstatement may remain undiscovered.

#### **Risk of Fraud and Error**

11. In planning and performing his examination the auditor should take into consideration the risk of material misstatement of the financial information caused by fraud or error. He should inquire of management as to any fraud or significant error which has occupied in the reporting and modify his audit procedures, if necessary.
12. In addition to weaknesses in the design of the internal control system and non-compliance with identified control procedures, conditions or events which increase the risk of fraud or error include:
  - (a) questions with respect to the integrity or competence of management;
  - (b) unusual pressures within an entity;
  - (c) unusual transactions;
  - (d) problems in obtaining sufficient appropriate audit evidence.

Examples of these conditions or events are set forth below.

#### **Procedures When There is an Indication That Fraud or Error May Exist**

13. If circumstances indicate the possible existence of fraud or error, the auditor should consider the potential effect on the financial information. If the auditor believes the suspected fraud or error could have a material effect on the financial information, he should perform such modified or additional procedures as he determines to be appropriate. The extent of such modifications or additional procedures depends on the auditor's judgment as to:
  - (a) the types of fraud or error that could occur;

(b) the relative risk of their occurrence;

(c) the likelihood that a particular type of fraud or error could have a material effect on the financial information.

14. Performing modified or additional procedures will normally enable the auditor to confirm or dispel a suspicion of fraud or error. Where confirmed, he should satisfy himself that the effect of fraud is properly reflected in the financial information or the error is corrected.

15. However, the auditor may be unable to obtain audit evidence either to confirm or dispel a suspicion of fraud. In this circumstance, the auditor should consider the possible impact on the financial information and the effect on his report. The auditor will also need to consider relevant laws and regulations and may wish to obtain legal advice before rendering any report on the financial information or withdrawing from the engagement.

16. Unless circumstances clearly indicate otherwise, the auditor should not assume that an instance of fraud or error is an isolated occurrence. If the fraud or error should have been prevented or detected by the system of internal control, the auditor should reconsider his prior evaluation of that system and, if necessary, adjust the nature, timing and extent of his substantive procedures.

17. When fraud or error involves a member of management, the auditor should consider the reliability of any representations made to the auditor by management.

#### **Other Reporting Responsibilities**

18. The auditor should communicate his findings to management on a timely basis if:

(a) he believes fraud may exist, even if the potential effect on the financial information would be immaterial; or

(b) fraud or significant error is actually found to exist.

In the latter circumstance, he should also consider his reporting responsibilities to regulatory authorities.

19.

In determining an appropriate representative of the entity to whom to report occurrences of possible or actual fraud or significant error, the auditor should consider all the circumstances. With respect to fraud, he should assess the likelihood of senior management involvement. In most cases involving fraud, it would be appropriate to report the matter to a level in the organization structure of the entity above that responsible for the persons believed to be implicated. When those persons ultimately responsible for the overall direction of the entity are doubted, the auditor should normally seek legal advice to assist him in the determination of procedures to follow.

#### **Examples of Conditions or Events Which Increase the Risk of Fraud or Error**

A. Questions with respect to the integrity or competence of management

(a) Management is dominated by one person (or a small group) and there is no effective oversight board or committee.

(b) There is a complex corporate structure where complexity does not seem to be warranted.

(c) There is a continuing failure to correct major weaknesses in internal control where such corrections are practicable.

(d) There is a high turnover rate of key accounting and financial personnel.

(e) There is significant and prolonged understaffing of the accounting department.

(f) There are frequent changes of legal counsel or auditors.

B. Unusual pressures within an entity

(a) The industry is declining and failures are increasing.

(b) There is inadequate working capital due to declining profits or too rapid expansion.

(c) The quality of earnings is deteriorating, for example, increased risk taking with respect to credit sales, changes in business practice or selection of accounting policy alternatives that improve income.

(d) The entity needs a rising profit trend to support the market price of its shares due to a contemplated public offering a takeover or other reason.

(e) The entity has a significant investment in an industry or product line noted for rapid change.

(f) The entity is heavily dependent on one or a few products or customers.

(g) Pressure is exerted on accounting personnel to complete financial statements in an unusually short time period.

#### C. Unusual transactions

(a) Unusual transactions, especially near the year-end, that have a significant effect on earnings.

(b) Transactions with related parties.

(c) Payments for services (for example, to lawyers, consultants or agents) that appear excessive in relation to the services provided.

#### D. Problems in obtaining sufficient appropriate audit evidence

(a) Inadequate records, for example, incomplete files, excessive adjustments to books and accounts transactions not recorded in accordance with normal procedures and out of balance control accounts.

(b) Inadequate documentation of transactions, such as lack of proper authorisation, supporting documents not available and alteration to documents (any of these documentation problems assume greater significance when they relate to large or unusual transactions).

(c) An excessive number of differences between accounting records and third party confirmations, conflicting audit evidence and unexplainable changes in operating ratios.

(d) Evasive or unreasonable responses by management to audit.

Factors unique to an EDP environment which relate to the conditions events in A through D above include:

- Inability to extract information from computer files due to lack of, or non-current documentation of records contents or programs.
- Large numbers of program changes that are not documented, approved and tested.
- Inadequate overall balancing of computer transactions and data bases to the financial accounts.