Fraud Control in Australian Government Entities

Better Practice Guide

March 2011
This Better Practice Guide was prepared by the Australian National Audit Office and KPMG.

ISBN No. 0 642 81180 6
© Commonwealth of Australia 2011

COPYRIGHT INFORMATION
This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Commonwealth.
Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth
Copyright Administration, Attorney-General’s Department, Robert Garran Offices, National Circuit, Canberra ACT 2600

Questions or comments on the Guide may be referred to the ANAO at the address below.
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601
Email: webmaster@anao.gov.au
Website: http://www.anao.gov.au
Foreword

Fraud continues to be an ever-present threat to the Australian community, posing significant challenges to organisations in its prevention and detection. Across business and government it has been estimated that only a third of fraud-related losses are actually being detected.¹

Sound and effective fraud control requires commitment at all organisational levels within an entity. Just as governance and project management arrangements have evolved to become common practice in government entities, fraud control strategies need to mature and become an accepted part of the day-to-day running of entities.

Recent deficiencies in the delivery of high-profile government programs resulted, in part, from a failure to implement robust fraud control measures early in the life cycle of these programs. This resulted in significant losses and reputational damage from fraudulent behaviour. A sound understanding by senior management of the responsibilities and expectations with regards to fraud control, can help ensure the Australian Public Service (APS) meets community expectations that government services and programs will be delivered with integrity.

In March 2011, the Minister for Home Affairs issued an updated version of the Commonwealth Fraud Control Guidelines (the Fraud Control Guidelines). These new guidelines are more principles-based, and establish the fraud control policy framework within which entities determine their own specific practices, plans and procedures to manage the prevention and detection of fraudulent activities.

This Better Practice Guide is intended to complement the Fraud Control Guidelines, and to augment the key fraud control strategies referred to in the Guidelines. While this Guide is an important tool for senior management and those who have direct responsibilities for fraud control, elements of this Guide will be useful to a wider audience, including employees, contractors and service providers. The Guide also takes account of the fact that fraud control arrangements need to be tailored to the individual entity’s circumstances.

The Guide has been prepared in consultation with the Attorney-General’s Department and should be read in conjunction with the Fraud Control Guidelines and the APS Values and Code of Conduct. The ANAO would like to acknowledge the assistance of KPMG in compiling this Guide, the Attorney-General’s Department in contributing to its content, and the entities that provided material for the case studies and input for other aspects of the Guide.

Ian McPhee
Auditor-General

¹. KPMG, Fraud and Misconduct Survey 2010.
IMPORTANT UPDATE
Introduction

1.1. The need for effective fraud control strategies

Fraud can be defined as ‘dishonestly obtaining a benefit by deception or other means’. Fraud control refers to the integrated set of activities to prevent, detect, investigate and respond to fraud and to the supporting processes such as staff training and the prosecution and penalisation of offenders.

Making sure that appropriate fraud controls are in place, continues to be an important function in Australian Government entities. Notwithstanding the financial and personal cost of fraud, the reputational damage to entities can be direct and long-lasting. Contemporary management in the Australian public sector is underpinned by managers and senior executives who are familiar with the key elements of a robust fraud control framework, including policy, legal and governance requirements.

Fraud control strategies based on a bi-annual preparation of a fraud control plan and fraud risk assessment are becoming less common. Increasingly, effective fraud control strategies are an integrated response led by the executive in an entity and embedded in its governance, program design and management. Such a proactive approach assists entities to manage fraud risk to an acceptable level, mindful of the changing landscape, source and types of fraud risk that must be assessed and managed.

1.1.1. Delivering services and programs in a changing landscape

An executive in today’s public sector is delivering programs and services in a changing and often challenging environment. Many Australian Government entities are responsible for administering significant levels of revenue, expenditure and property, and because these activities involve contact with a broad range of clients and citizens, there is an increasing reliance on technology and e-commerce. These advances in the use of technology are making identity fraud one of the fastest growing crimes in Australia. In this environment, the prevention and detection of fraud is critical.

The application of sound governance to fraud control is required to keep pace with the growing convergence of the public and private sectors. The step-up in the strategic partnerships and a greater emphasis on outsourcing of government services is creating a new environment of fraud risk, that of fraud by service providers. Fraud control strategies must extend to these outsourced arrangements, partnerships and alliances through effective contract management and strong relationships.

1.1.2. Effective program design and management

The emerging focus on responsive and flexible programs to meet community and industry expectations can expose the Commonwealth to internal and external fraud risks. For instance, the demand for timeliness and flexibility in service delivery can create new challenges in maintaining the integrity of programs. The emergence of these types of fraud risks reinforces the imperative for entities to consider fraud control at each critical stage of a program’s life cycle.

2. Attorney-General’s Department, Commonwealth Fraud Control Guidelines, Canberra, 2011.
3. In broad terms ‘entity’ is used to refer collectively to Australian government departments and other government bodies. The distinctions between the types of government entities and relevance to fraud control are set out in Chapter 3.
1.1.3. Perpetrators of fraud

The risk of fraud can come from inside an organisation, that is, from its employees or contractors, or from outside an organisation, that is, external parties such as clients, consultants, service providers or other members of the public. Organisations must be alert to the risk of fraud through collusion between employees and external parties (bribery, corruption and abuse of office are examples of this type of fraud). In addition, recent fraud response activities have identified that elements of organised crime are viewing government programs as potential targets for systematic rorting and abuse.

1.2. Legislative and policy requirements

The Australian Government is committed to protecting its revenue, expenditure and property from fraudulent activity by taking a systemic approach to the management of fraud across the Australian Public Service (APS). This commitment is articulated in the provisions of the Financial Management and Accountability Act 1997 (the FMA Act) and the Commonwealth Authorities and Companies Act 1997 (CAC Act).

1.2.1. Commonwealth Fraud Control Guidelines

The Australian Government first released a Commonwealth Fraud Control Policy in 1987. In 2002, the government recognised the need to update the policy to take into account developments in corporate governance, modern business practices and developments in fraud control. Accordingly, the then Minister for Justice and Customs issued the Commonwealth Fraud Control Guidelines (the Fraud Control Guidelines) under Regulation 19 of the Financial Management and Accountability Regulations 1997.

Following a review in 2010, the Minister for Home Affairs issued an updated version of the Fraud Control Guidelines in March 2011. The Fraud Control Guidelines establish the fraud control policy framework within which entities determine their own practices, plans and procedures to manage the prevention and detection of fraudulent activities within their organisation, and the investigation and, where appropriate, prosecution of offenders.

1.3. Who will benefit from the Guide?

This Guide is directed at a wide set of stakeholders who carry responsibility for the effective and efficient control of fraud risks, both inside and outside the Australian Government.

**Senior executives**

The Guide has been developed with the first four chapters being intended as a source of guidance for senior executives. These introductory chapters provide the legislative and policy framework for fraud control in Australian Government entities; set the tone for leadership, culture and integrity; and summarise the key strategies necessary to ensure best practice fraud control is embedded in organisational governance and processes.

**Fraud Managers**

Fraud Managers have delegated responsibility for fraud control within their organisation. This Guide is a key reference document to support the Fraud Manager’s day-to-day business.
**Operational managers**
Those operational managers with responsibility for fraud control strategies, such as analysis of management accounting reports or conducting compliance reviews, should use this document on a regular basis as a reference point.

**Line area employees**
Because fraud control is the responsibility of all employees, this Guide will be useful in highlighting the importance of ethics and integrity, and raising awareness of how internal fraud controls, such as fraud reporting channels, can help reduce fraud risks.

**Service providers and contractors**
The Fraud Control Guidelines point out that effective fraud control requires the commitment of all contractors and external service providers. This Guide will assist in raising awareness of the better practice principles the Australian Government expects from contractors and service providers with respect to fraud control.

### 1.4. Purpose and structure of the Guide

This new Guide reflects the changing fraud risk landscape and explains what is involved in establishing a sound fraud control environment. The Guide updates the ANAO’s 2004 Fraud Control Better Practice Guide and includes case studies and practical examples to assist entities to improve their fraud control practices.

The Fraud Control Framework is illustrated in Figure 1.1. The framework is consistent with the Commonwealth’s legislative and policy requirements and is based on governance models and fraud control strategies which are considered best practice in the public and private sectors.

The body of the Guide is organised around the elements of the fraud control framework, as depicted in sequence below.

**Figure 1.1: Fraud control framework**

---

Setting the right ‘tone at the top’ is critical to fraud control in Australian Government entities. An organisational culture based on sound ethics and integrity is an essential ingredient that underpins effective fraud control.

The legislative framework for fraud control in Australian Government is supported by a number of key policies. Rigorous governance structures and processes help ensure the requirements of these policies and legislation are operationalised in an accountable, effective and transparent way.

Central to better practice fraud control are key control strategies which contribute to an effective fraud control framework. These strategies are interdependent and subject to a cyclic process of review and enhancement.
**Case studies**

The Guide includes case studies and practical examples to assist entities to improve their fraud control practices. The Guide recognises that fraud control arrangements will vary according to an organisation’s role, size, functions and particular characteristics, especially its fraud risk profile.

**Program management**

Because of the growing emphasis on program delivery in the Australian Government, the Guide provides program-specific assistance on how to manage fraud risks at each critical stage of the program life cycle. This assistance is provided throughout the Guide, in context with the pertinent fraud control strategies.

**Identity fraud**

Identity fraud is one of the fastest growing crimes in Australia and costs the Australian community billions of dollars every year. Guidance on initiatives to combat the rapidly emerging problem of identity fraud is provided in a dedicated chapter.
Leadership and Culture

Key points

▷ Strong executive leadership is integral to effective fraud control within organisations.

▷ If staff perceive that controls to respond to fraud are not robust or supported by management, they are much less inclined to report their observations or suspicions.

▷ To keep astride of emerging fraud risks there needs to be a shift from ‘traditional’ fraud control to ‘contemporary’ fraud control.

▷ The establishment of an ethical culture is a key element of sound governance and plays an important role in preventing fraud and helping to detect it once it occurs.
2.1. Leadership

The realisation of fraud risks in a number of high-profile government programs has resulted in a heightened expectation that fraud risks will be given appropriate attention in the management of public sector entities. For this reason, there has been renewed focus on strong and executive leadership to support effective fraud control within organisations. Poor leadership can lead to a culture of complacency within organisations with respect to fraud control and management.

Managers are required to demonstrate an observably high level of commitment to the control of fraud. Balancing fraud control with other high-level corporate and operational responsibilities can be challenging for executives. An effective organisational governance structure, with clearly defined roles and accountabilities for individuals and decision-making bodies (for example, the Audit Committee, Executive Board or Program Management Committee), can assist.

A ‘top-down’ and ‘bottom-up’ approach to fraud control can help ensure an organisation’s policies, governance structures and processes for managing fraud risks are consistent and mutually reinforcing. Senior executives are best placed to understand whole-of-organisation issues and risks, and to provide a broad context to fraud risk assessments and fraud monitoring and evaluation exercises. Table 2.1 provides the types of considerations for an Executive to be suitably engaged in their organisation’s fraud control strategies.

Table 2.1: Considerations for an Executive suitably engaged in fraud control

<table>
<thead>
<tr>
<th>Who</th>
<th>Who reviews and evaluates the fraud control plan?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Who hasn’t done the fraud awareness training?</td>
</tr>
<tr>
<td></td>
<td>Who analyses the fraud risks in my organisation / program?</td>
</tr>
<tr>
<td>What</td>
<td>What are the drivers of fraud risk at the organisation and program level?</td>
</tr>
<tr>
<td></td>
<td>What is my role in fraud control?</td>
</tr>
<tr>
<td></td>
<td>What is a proportionate response to fraud risks in my organisation / program?</td>
</tr>
<tr>
<td>When</td>
<td>When do I get involved in fraud prevention and detection strategies?</td>
</tr>
<tr>
<td></td>
<td>When do we report fraud in the organisation?</td>
</tr>
<tr>
<td></td>
<td>When do we analyse fraud activity?</td>
</tr>
<tr>
<td>Where</td>
<td>Where can I find my organisation’s Fraud Policy?</td>
</tr>
<tr>
<td></td>
<td>Where is the guidance on how to report fraud in my organisation / program?</td>
</tr>
<tr>
<td></td>
<td>Where can I refer matters of serious and complex fraud?</td>
</tr>
<tr>
<td>Why</td>
<td>Why is our organisation / program at risk of fraud?</td>
</tr>
<tr>
<td></td>
<td>Why is governance so important to effective fraud control?</td>
</tr>
<tr>
<td></td>
<td>Why weren’t our fraud risks reviewed when our organisation structure changed?</td>
</tr>
<tr>
<td>How</td>
<td>How do I get assurance that fraud risks are addressed in program design?</td>
</tr>
<tr>
<td></td>
<td>How do I know our fraud strategies are working in my organisation / program?</td>
</tr>
<tr>
<td></td>
<td>How does my organisation decide if a suspected fraud will be investigated?</td>
</tr>
</tbody>
</table>

Recent studies have identified that a lack of leadership in fraud prevention, detection and response can reduce the likelihood of fraud being reported to management. If staff perceive that controls to respond to fraud are not robust or supported by management, they are much less inclined to report their observations or suspicions.5

---

To keep astir of emerging fraud risks there needs to be a shift from ‘traditional’ fraud control to ‘contemporary’ fraud control (as described below). To achieve this goal, Australian Government entities will be required to embed key elements of fraud control in organisational governance, leadership and culture. This can be made possible through senior strategic oversight and leadership, and through effective use of this Guide. Table 2.2 illustrates what is required to shift from traditional to contemporary fraud control.

### Table 2.2: Traditional vs. contemporary fraud control

<table>
<thead>
<tr>
<th>Traditional fraud control</th>
<th>Contemporary fraud control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud risk assessment is a static document only updated every two years.</td>
<td>Fraud risk assessment is a living document which is updated through regular, targeted risk assessments.</td>
</tr>
<tr>
<td>Fraud control plan is updated and ‘filed’ until the next biennial review.</td>
<td>Ongoing fraud control where the fraud control plan is a living document, which is updated in lieu of fraud risk assessments.</td>
</tr>
<tr>
<td>Fraud control plan is owned and managed by the Fraud Manager.</td>
<td>Fraud control plan is ‘owned’ by the Executive. An entity’s Audit Committee provides independent assurance and advice to the CEO / Board on the operation of key controls and the fraud control plan to the extent that it is within its charter. The fraud control plan is managed by the Fraud Manager and referenced by all levels of management.</td>
</tr>
<tr>
<td>Program development and delivery is not referenced by the fraud control plan, and programs do not consider fraud control at key stages in the program life cycle.</td>
<td>Fraud control plan informs fraud risk assessment and fraud control strategies for key stages in the program life cycle, particularly in program design.</td>
</tr>
<tr>
<td>Fraud awareness training is delivered to new staff members at induction.</td>
<td>Fraud awareness training is sponsored by the Senior Executive and conducted regularly under a risk-based approach.</td>
</tr>
</tbody>
</table>

### 2.2. An ethical culture

The establishment of an ethical culture is a key element of sound governance and plays an important role in preventing fraud and helping to detect it once it occurs. The Public Service Act 1999 highlights the need for an ethical culture and also sets out the APS Values and Code of Conduct. These provide mandatory requirements for all APS employees to uphold the Values and to comply with the Code of Conduct.

While the Values and the Code of Conduct provide a commonly understood set of principles for APS employees, each entity must reinforce the intent of these documents through active management strategies. The Australian Public Service Commissioner provides a checklist to assist senior executives to assess how well the APS Values and Code of Conduct are being integrated into the management and culture of an entity.6

---

Questions on this checklist include the following.

- In what ways do senior leaders demonstrate visible and strong commitment to the APS Values?
- How do senior leaders communicate to employees that conduct consistent with the APS Values and Code of Conduct is expected and that misconduct will not be tolerated?
- Are there learning and development programs available to all employees that: address their responsibilities under the APS Values and Code of Conduct, handling tensions inherent in the APS Values; develop skills for ethical analysis and reasoning; and provide sources of guidance and direction?
- Are all instructions and guidance to employees, including chief executive instructions, people management rules and guidance, and advice on communications with ministers’ offices and the media, consistent with and supportive of the APS Values and Code of Conduct?
- What measures are in place to ensure that internal control systems, such as internal audit, fraud control strategies and risk assessment, are functioning and effective?

Senior executives must ensure the work practices of their organisations are consistent with the principles of the APS Values and Code of Conduct. Creating a culture in which employees are prepared to report a suspected fraud and supported when they do so is critical in the ongoing operation of an organisation’s fraud control strategy. In terms of fraud detection, the KPMG Fraud and Misconduct Survey 2010 identified that 20 per cent of reported major frauds were identified by employees. The Australian Institute of Criminology has also reported that the detection of external fraud through discovery by staff members or colleagues was an important method of detection.

---


Sections 14 and 41 of the Financial Management and Accountability Act 1997 make it a criminal offence for a Commonwealth officer to misapply, improperly dispose of, or use public money or property.

Section 26 of the Commonwealth Authorities and Companies Act 1997 makes it a criminal offence for officers of a Commonwealth authority to use their position dishonestly with the intention of gaining a personal advantage, to the detriment of the Commonwealth authority.

The Fraud Control Guidelines establish a fraud control policy framework for Australian Government entities.

Fundamental to sound fraud management is an overall governance structure that appropriately reflects the operating environment of an entity.

An entity’s Audit Committee plays a key role in securing and enhancing awareness of fraud control across an organisation, including reviewing management’s approach to new and emerging risks during periods of significant change, such as the implementation of new policies and programs.
The Australian Government is committed to protecting its revenue, expenditure and property from fraudulent activity by taking a systemic approach to the management of fraud across the Australian Public Service. This commitment is articulated in the legal provisions of the:

- Financial Management and Accountability Act 1997 (FMA Act); and

The government’s fraud control policy requirements for FMA Act agencies and CAC Act bodies are outlined in the Commonwealth Fraud Guidelines 2011 (Fraud Control Guidelines).9

The following sections set out: key elements of the legal and policy framework; the responsible central agencies within the Attorney-General’s portfolio; and appropriate governance structures for entities.10

3.1. Legal framework

3.1.1. FMA Act

The FMA Act covers agencies which are legally and financially part of the Commonwealth, and specifies the responsibilities and powers of Chief Executive Officers (CEOs) and officials, including the responsibilities associated with the expenditure of public monies. Section 44 of the FMA Act requires a CEO to manage the affairs of the agency in a way that promotes the efficient, effective, and ethical use of the Commonwealth resources for which the CEO is responsible. This legislation places the onus on CEOs to promote ethical behaviour in their agencies and recognises that leading from the top is important in establishing the ethical tone in an organisation.

Provisions of the FMA with particular relevance to fraud are sections 14 and 41, which make it a criminal offence for a Commonwealth officer to misapply, improperly dispose of, or use public money or property.

3.1.2. Public Service Act 1999—APS Values and Code of Conduct

The Public Service Act 1999 (Public Service Act) also supports the government’s policy regarding the ethical behaviour of officials in the APS. The APS Values, described in section 10 of the Public Service Act, provide the philosophical underpinning of the APS and articulate its culture and ethos. The APS Values reflect the Australian community’s expectations of public servants and are directly relevant to the roles and functions of government, such as administration of revenue, expenditure and property and other core functions of government including policy development and review. The Public Service Act requires that APS employees at all times behave in a way that upholds the APS Values and the integrity and good reputation of the APS.11 The APS Values require employees to: have the highest ethical standards; be openly accountable; and deliver services fairly, effectively, impartially and courteously.

The APS Values are complemented by the requirements of the APS Code of Conduct, which is set out in section 13 of the Public Service Act. Among other things, the Code requires that all APS employees:

- behave honestly and with integrity in the course of their employment in the APS;

---

9. Appendix A lists the key elements of the Australian Government’s legislation, policies and guidelines relevant to fraud control.
10. In this document, ‘FMA Act agencies’ and ‘CAC Act bodies’ are specifically referred to, where appropriate. As noted previously, the term ‘entities’ is used to refer to both types of organisations collectively.
• disclose, and take reasonable steps to avoid, any conflict of interest (real or apparent) in connection with their employment in the APS;

• use Commonwealth resources in a proper manner;

• not make improper use of inside information or the employee’s duties, status, power or authority in order to gain, or seek to gain, a benefit or advantage for the employee or for any other person; and

• at all times behave in a way that upholds the APS Values and the integrity and good reputation of the APS.

The Public Service Act provides for the imposition of sanctions on APS employees found to have breached the APS Code of Conduct. Possible sanctions include: termination of employment; reduction in classification; re-assignment of duties; reduction in salary; deductions from salary, by way of fine; or a reprimand.

Figures 3.1 below illustrates the legislative and policy framework for FMA Act agencies.

Figure 3.1: Legal and policy framework for fraud control in FMA Act agencies

Source: KPMG.
3.1.3. CAC Act

The CAC Act applies to Commonwealth authorities and Commonwealth companies. Commonwealth authorities are bodies corporate that are established by legislation for a public purpose and which hold money on their own account (that is, for their own purposes). Commonwealth companies are companies incorporated under the Corporations Act 2001 that the Commonwealth controls. CAC Act bodies are legally and financially separate from the Commonwealth.

The CAC Act imposes a number of obligations on officers and employees of Commonwealth authorities to exercise care and diligence and to act in good faith. As well as this general duty of care, the CAC Act imposes a number of additional obligations. For example, an officer or employee of a Commonwealth authority must not:

- improperly use his or her position to gain an advantage for him or her or someone else (section 24(1));
  and / or
- improperly use information obtained as an officer or employee of a Commonwealth authority to gain advantage for him or her or someone else or cause detriment to the Commonwealth authority or to another person (section 25(1)).

In addition, an officer of a Commonwealth authority must exercise his or her powers and discharge his or her duties in good faith in the best interests of the Commonwealth authority and for a proper purpose. An officer or employee of a Commonwealth authority may be liable to criminal sanctions where these obligations are breached (section 26).

The CAC Act also contains rules relating to the disclosure of conflicts of interest by directors of a Commonwealth authority. For example:

- a director of a CAC Act entity who has a material personal interest in a matter that relates to the affairs of the authority must give other directors notice of this interest (section 27F(1)). Subject to specific conditions, a director who has a material personal interest in a matter that is being considered at a directors’ meeting, must not be present while the matter is being considered (section 27J(1)).

3.1.4. Overall expectations

While the legal and compliance obligations of FMA Act agencies and CAC Act bodies can differ, the Australian community expects business in the public sector to be conducted ethically, displaying honesty, integrity, diligence, fairness, trust, and respect when dealing with others. For these reasons it is advisable that entities, (whether FMA Act agencies or CAC Act bodies), put mechanisms in place to assist and train their staff to understand ethical issues and develop the judgment and skills needed to deal appropriately with fraud or other misconduct.

3.1.5. Prosecution

While fraud against the Commonwealth may be prosecuted under a number of different Commonwealth laws, Part 7.3 of the Criminal Code Act 1995 specifically deals with fraudulent conduct against the Commonwealth and contains a range of criminal offences for fraud. These offences may apply to APS employees, service providers and contractors, or other members of the public.

---

The offences provided in Part 7.3 of the *Criminal Code Act 1995* include:

- dishonestly obtaining a financial advantage from a Commonwealth entity by deception;
- doing anything with the intention of dishonestly obtaining a gain from a Commonwealth entity, or causing a loss to a Commonwealth entity; and
- dishonestly influencing a public official in the exercise of their duties.

### 3.2. Commonwealth Fraud Control Guidelines—
the policy framework

The Australian Government first released its fraud control policy in 1987. Following a review in 2010, the Minister for Home Affairs issued new Fraud Control Guidelines in March 2011. The Fraud Control Guidelines establish the fraud control policy framework within which entities determine their own specific practices, plans and procedures to manage the prevention and detection of fraudulent activities within their organisation, and the investigation and, where appropriate, prosecution of offenders.

#### 3.2.1. Applicability of the Fraud Control Guidelines

The purpose of the Fraud Control Guidelines is to establish the policy framework and articulate the government’s expectations for all FMA Act agencies and relevant CAC bodies.

The Fraud Control Guidelines were issued under Regulation 19(1) of the *Financial Management and Accountability Regulations 1997*. Regulation 19(2) requires officials to have regard to the Fraud Control Guidelines when performing duties related to the efficient, effective and ethical management of public resources.

Compliance with the Fraud Control Guidelines is also required by those CAC Act bodies that have received a General Policy Order (made under section 48A of the CAC Act) from the Minister for Finance and Deregulation that the Fraud Control Guidelines apply to them. That said, the Fraud Control Guidelines state that, where a General Policy Order does not apply to a CAC Act body, the body should consider applying the Fraud Control Guidelines as a matter of policy and better practice.

#### 3.2.2. Definition of fraud

For the purpose of the Fraud Control Guidelines, fraud against the Commonwealth is defined as ‘dishonestly obtaining a benefit by deception or other means’. A benefit is not restricted to monetary or material benefits, and may be tangible or intangible. A third party may also obtain a ‘benefit’ rather than, or in addition to, the perpetrator of the fraud.

#### 3.2.3. Objectives of the Fraud Control Guidelines

The Fraud Control Guidelines are part of the Australian Government’s broader financial management framework, which creates an overarching requirement to manage an entity’s affairs efficiently, effectively and ethically and in accordance with the policies of the Commonwealth. The objectives of the Fraud Control Guidelines are to:
- protect public money and property; and protect the integrity and good reputation of Commonwealth entities.
- This includes reducing the risk of fraud occurring, discovering and investigating fraud when it occurs, and taking corrective action appropriate to the degree of fraudulent behaviour.
3.3. The role of central agencies

The Attorney-General’s Department

The Attorney-General’s Department is responsible for providing high-level policy advice to the government about fraud control arrangements within the Commonwealth. This includes developing and reviewing general policies of government with respect to fraud control, currently embodied in the Fraud Control Guidelines, and advising Commonwealth entities about the content and application of those policies.

The Australian Institute of Criminology

The Australian Institute of Criminology is responsible for conducting an annual fraud survey of Australian Government entities and producing a report on fraud against the Commonwealth, and fraud control arrangements within Australian Government entities. This ‘in-confidence’ report is known as the Annual Report to Government: Fraud against the Commonwealth and, as mandated by the Fraud Control Guidelines, is to be provided to the Minister for Home Affairs.

The Australian Federal Police

The Australian Federal Police investigates serious or complex crime against Commonwealth laws, its revenue, expenditure and property. Such crime can include both internal fraud and external fraud committed against the Commonwealth. Internal fraud is fraud perpetrated by an employee or contractor of an organisation. External fraud is fraud perpetrated by a customer, external service provider or third party.

The Commonwealth Director of Public Prosecutions

The Commonwealth Director of Public Prosecutions is responsible for prosecuting offences against Commonwealth law and for conducting related criminal assets recovery. All prosecutions and related decisions are made in accordance with the guidelines set out in the Prosecution Policy of the Commonwealth.

The Australian National Audit Office

The ANAO’s mandate extends to all FMA agencies, CAC Act bodies and subsidiaries, with the exception of the conduct of performance audits of government business enterprises and of persons employed or engaged under the Members of Parliament Act 1994.

The mandate includes the audit of the annual financial statements of FMA agencies, CAC Act bodies and subsidiaries. Financial statements may be misstated due to fraud or error. In accordance with Australian auditing standards, the ANAO’s financial statement audits include the identification and assessment of the risks of material misstatement of the financial statements due to fraud and the obtainment of sufficient, appropriate audit evidence regarding these assessed risks through its audit procedures. In these audits the ANAO is concerned primarily with two types of fraud, these being misstatements resulting from misappropriation of assets and misstatements resulting from fraudulent financial reporting.

The ANAO also conducts performance audits that evaluate the efficiency and administrative effectiveness of Commonwealth public sector entities within its mandate. This may involve an examination of governance arrangements including risk management and other control structures, resource use, information systems, performance measures, reporting and monitoring systems, and legal compliance. Performance audits may from time to time be undertaken to examine the operations of entities’ fraud control arrangements to prevent, detect and respond to fraud.\(^{13}\)

---

\(^{13}\) Appendix D lists recent ANAO audits related to fraud control.
3.4. Governance structures

Fundamental to sound fraud management is an overall governance structure that appropriately reflects the operating environment of an entity. An effective organisational control structure, which includes fraud control, will assist an entity to promote ethical and professional business practices, improve accountability, and contribute to quality outcomes.

When developing or maintaining a fraud control governance structure, an entity needs to ensure it has formally considered the three generally recognised conditions for fraud to occur: the presence of an opportunity (that is, poor internal and external controls); a motivated offender; and rationalisation (justification by the individual for the fraudulent activity).

To minimise these conditions occurring, fraud control measures need to be primarily focused on restricting the level of opportunity available to potential fraudsters through the development and implementation of an effective fraud control framework. The leadership demonstrated by the senior executives of an entity plays an important role with respect to fraud control, and along with the organisational culture of an entity, are the primary controls to minimise these conditions occurring. Important elements for effective fraud control include: governance structures; organisational values and culture; and fraud control strategies.

Appropriate governance structures are critical to the effective operation of fraud control within an entity and support the role of the CEO and compliance with the Fraud Guidelines. These governance structures need to be well understood and accepted by the organisation.

**Chief Executive Officer or Secretary (FMA Act agency)**

The CEO or Secretary of an FMA Act agency is accountable for fraud control within that agency and is responsible for ensuring that adequate fraud controls are in place to comply with the Fraud Control Guidelines. This includes the need to ensure that a sound control framework and governance mechanisms exist and are effective in supporting fraud control activities.

**The Board and Chief Executive Officer (CAC Act body)**

The directors of the Board of a CAC Act body have primary accountability for fraud control, ensuring that appropriate governance mechanisms and fraud control frameworks are in place and operating as designed. The CEO of a CAC Act body is accountable for fraud control within that body and is responsible for ensuring the sound operation of the control environment, governance mechanisms and the fraud control activities.

**Executive leadership**

Strong executive leadership from management is integral to effective fraud control within an entity. Managers should demonstrate an observably high level of commitment to fraud control and the management of fraud, in addition to ensuring that business processes and internal and external controls are planned and undertaken following the due consideration of fraud risk exposures. Managers should also ensure that adequate frameworks are established to support the monitoring and reporting of fraudulent activities and progress in pursuing fraud control strategies.

**Fraud Manager**

Clear lines of responsibility in relation to the co-ordination, monitoring, review and promotion of the fraud control framework need to be established within an entity. This can include the appointment of a central point of contact for all fraud-related matters. This central point of contact is often referred to as the ‘Fraud Manager’.
A Fraud Manager is the individual with delegated responsibility from the CEO / Board for fraud control within an entity. A Fraud Manager’s responsibilities need to be articulated in a fraud control plan and understood by the entity at large. Where such a position is employed, an appropriate line of reporting is directly to the CEO / Board.

Larger entities, or entities with higher levels of fraud risk, may also establish a specialised in-house fraud unit to support the Fraud Manager. Fraud units are typically responsible for fraud prevention, detection and response activities.

**Audit Committee**

An entity’s Audit Committee plays a crucial role in providing independent assurance and advice to the CEO / Board on the entity’s operations, its control regime and its adherence to statutory requirements. Key responsibilities of audit committees include:

- risk management;
- the internal control framework;
- external accountability (including the entity’s financial statements);
- legislative compliance;
- internal audit; and
- external audit.

An audit committee’s responsibilities in relation to fraud control would generally include:

- reviewing management’s risk management framework and associated procedures for the effective identification and management of the entity’s financial and business risks, including fraud risks; and
- overseeing the process of developing and implementing the fraud control plan, to provide assurance that the entity has appropriate processes and systems in place to prevent, detect and effectively respond to fraud-related information.

In some entities, a sub-committee of the Audit Committee may exist which has fraud control as one of its key oversight responsibilities. Typically these sub-committees are in entities with large benefit payment programs where business integrity activities are critical and require active management.

---

14. Further information on the role and function of an Audit Committee is available in the ANAO Better Practice Guide—Public Sector Audit Committees – Having the right people is the key, 2005. The ANAO intends to update this Better Practice Guide in 2011.
Department of Veterans’ Affairs Integrity Sub-committee

The Department of Veterans’ Affairs (DVA) has established a sub-committee of its Audit and Risk Committee known as the Integrity Sub-committee. The sub-committee focuses on a range of matters which includes:

• reviewing DVA’s fraud control plan, and providing assurance to the Audit and Risk Committee that DVA has appropriate policies, processes and systems in place to capture and effectively investigate fraud-related information;

• monitoring DVA’s approach to suspected fraud investigations and case management;

• reviewing whether management has taken steps to embed a culture which is committed to ethical and lawful behaviour; and

• monitoring adherence to, and potential breaches of, DVA’s integrity framework and the internal code of conduct.

Like the Audit and Risk Committee, the Integrity sub-committee has an independent member. Other members of the Committee have sufficient, relevant, executive authority to deal with operational issues, should they arise.

Appendix B provides an aide-memoir designed to assist an Audit Committee’s consideration of fraud control through the review of material, discussion or presentations from senior management. This aide-memoir consists of a series of questions, or high-level prompts, which should be tailored to meet the entity’s particular circumstances.

Internal audit

Internal audit provides an independent and objective review and advisory service to:

• provide assurance to the CEO / Board that the financial and operational controls designed to manage the entity’s risks and achieve the entity’s objectives are operating in an efficient, effective and ethical manner; and

• assist management in improving the entity’s business performance.15

Internal audit can specifically assist an entity to manage fraud control by providing advice on the risk of fraud, advising on the design or adequacy of internal controls to minimise the risk of fraud occurring, and by assisting management to develop fraud prevention and monitoring strategies.

An effective internal audit plan should include a review of those fraud controls designed to address the significant fraud risks faced by an entity.

3.4.1. Linking fraud control across governance structures

Fraud control and its operation within an entity needs to form part of its overall governance framework. Owing to its nature and separate statutory reporting requirements, fraud control can often operate in isolation within an entity. An entity’s audit committee can play a key role in securing awareness that fraud control interacts and links with other governance frameworks across the entity. This understanding provides for fraud and its possible impacts to be considered at appropriate times when significant changes or decisions occur, for example the implementation of new policies and programs. Figure 3.2 illustrates how a governance structure might be arranged for fraud control in an entity.

**Figure 3.2: Fraud control governance structure**

Practical examples of linking fraud control across governance structures include:

- Linking the update of the fraud risk assessment to the update of the entity’s risk assessment and business planning processes. This ensures fraud and its possible consequences can be formally considered in context with other significant risks facing the entity.

- Formalising the relationship between fraud control and the operation of any compliance strategies that an entity has in place. This ensures the compliance strategies are informed by the outcomes of the entity’s fraud risk assessment and fraud control plan.
# BETTER PRACTICE CHECKLIST

**Fraud control governance arrangements**

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the entity have an effective and articulated fraud control framework in place?</td>
<td></td>
</tr>
<tr>
<td>Does the entity have a central point of contact for fraud control within the entity?</td>
<td></td>
</tr>
<tr>
<td>Does the Audit Committee have a role in overseeing the development and implementation of the fraud risk assessment and fraud control plan?</td>
<td></td>
</tr>
<tr>
<td>Is information on the entity’s values and code of conduct easily accessible to employees and included as part of its induction processes?</td>
<td></td>
</tr>
<tr>
<td>Does the entity have a conflict of interest policy and is this easily accessible and understood by employees?</td>
<td></td>
</tr>
</tbody>
</table>
Fraud control requires the implementation of a number of key control strategies which contribute to an effective fraud control framework. These strategies are interdependent and subject to a cyclic process of review and enhancement. The strategies are grouped in four key themes.

For these strategies to be effective in the context of an overarching fraud control framework, each strategy must be subject to active management and ownership within an organisation.

For most government programs, the prevention, detection and response elements of the fraud control framework will need to be considered at each stage of the program. The key is to get the right balance between fraud risk and control, and to manage the fraud risks while maximising and enhancing operational performance.
4.1. Key fraud control themes

Fraud control requires the implementation of a number of key control strategies which contribute to an effective fraud control framework. These strategies are interdependent and subject to a cyclic process of review and enhancement. The strategies are grouped in four key themes:

- **Fraud prevention** involves those strategies designed to prevent fraud from occurring in the first instance;
- **Fraud detection** includes strategies to discover fraud as soon as possible after it has occurred;
- **Fraud response** covers the systems and processes that assist an entity to respond appropriately to an alleged fraud when it is detected; and
- **Fraud monitoring, reporting and evaluation** are strategies to provide assurance that legislative responsibilities are being met, as well as promoting accountability by providing information that demonstrates compliance with specific fraud control strategies.

For these strategies to be effective in the context of an overarching fraud control framework, each strategy must be subject to active management and ownership within an organisation. Senior executive oversight through sound governance arrangements will ensure that each strategy does not operate in isolation, and that interdependencies are effectively identified and managed appropriately.

The following four chapters provide better practice strategies, systems and processes associated with each fraud control theme described above.

4.2. Fraud control strategies and program management

Government entities are regularly required to develop and implement programs to facilitate the delivery of services or stimulus to specific sections of the community. Often these programs support the establishment or delivery of new government services and/or payments. Whenever programs are developed, new opportunities to perpetrate fraud may arise, giving rise to the need for an entity to consider the threat of fraud to the program. This fraud is likely to be from parties both internal and external to an organisation.

4.2.1. Strategic fraud control

The implementation of a new program provides entities with a challenge in balancing the need to deliver the program in an efficient and effective way, with its regulatory responsibilities relating to the proper use of public monies and the Fraud Control Guidelines.

Managing the risk of fraud in a program context typically involves its consideration at each critical stage of the program life cycle. The critical stages of a program generally relate to its: design and business case; procurement strategy; delivery / implementation / management; and closure.

The risk of fraud should also be considered at the policy development stage. This is particularly relevant where the features of a new government policy or program affect the inherent capacity of the initiative to be delivered with a high level of integrity. Factors that affect the potential for fraudulent activity include the degree of flexibility in the eligibility rules and the schedule of services to be provided.

In such cases, the risk of fraud will need to be assessed against desirable aspects of successful program implementation, such as timeliness, accessibility, and the level of personal information required from recipients.
Where the risk of fraud is high, it will be appropriate to introduce preventative controls, such as increased requirements for personal and other relevant information to establish eligibility and the appropriate level of payment, in order to reduce the potential for fraud.

The method of delivery of a government policy or program can also affect the risk of fraud. For example, approaches to deliver government services increasingly use third-party providers and make greater use of e-commerce, including the internet. While these arrangements provide for ease of access to government services, they may also increase the government’s exposure to fraud.

For most programs, the prevention, detection and response elements of the fraud control framework will need to be considered at each stage of the program. The key is to get the right balance between fraud risk and control, and to manage the fraud risks while maximising and enhancing operational performance.

For many organisations, the resources available may be limited relative to its fraud control responsibilities. As such, each entity needs to plan at both a strategic and operational level to best meet its responsibilities within its allocated resources and budget. This means planning its fraud control activities based on addressing priority areas and providing for a method of measuring the outcomes of those activities, in terms of their success or otherwise, in meeting its primary objectives. For fraud control purposes, the focus is on reducing the level of fraud in the program through integrated strategies around prevention, detection and response.

**4.2.2. Examples of program-specific fraud controls**

The type and quantity of fraud controls that can be established within a program generally depend on the objective of the program and the mechanisms it uses to achieve its aim. Table 4.1 below has been structured against the typical life cycle of a program and provides some examples of fraud controls that could be used in a program.

**Table 4.1: Examples of fraud controls at typical life cycle phases of a program**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Examples of fraud controls</th>
</tr>
</thead>
</table>
| Policy development, program design and business case | • Fraud risk assessment  
• Fraud control plan  
• Employment screening  
• Communication and awareness |
| Procurement strategy | • Rigorous and transparent tender processes  
• Screening of potential suppliers and customers  
• Segregation of duties on selection and approval of procurements |
| Delivery / implementation / management | • Regular supplier reviews (includes surprise audits)  
• Data mining / analysis  
• Internal and external reporting mechanisms (hotlines, website, internal reporting channels)  
• Response to identified / reported frauds  
• Management / internal audit review of internal controls |
| Closure | • Management / internal audit review of program closure and expenditure of final monies |
Key points

- Fraud prevention strategies are the first line of defence and provide the most cost-effective method of controlling fraud within an entity.

- Risk management is crucial to fraud control as it guides the development of an effective fraud control plan.

- A fraud policy statement assists employees to understand what fraud is, their organisation’s attitude to fraud, and what to do if they suspect fraud is being perpetrated.

- In determining a ‘fit for purpose’ approach to managing fraud risks, the resources devoted to preventative strategies should be proportionate to the fraud risk profile.

- Providing information to employees and customers on fraud detected and action taken indicates that there are consequences attached to committing fraud and this can act as an effective deterrent.

- A separate fraud risk assessment and fraud control plan can be considered for large or high-risk programs in order to address the fraud risk applicable to the program.
Fraud prevention strategies are the first line of defence and provide the most cost-effective method of controlling fraud within an entity. To be effective, fraud prevention within an organisation requires a number of contributory elements, including an ethical organisational culture, a strong awareness of fraud among employees, suppliers and clients, and an effective internal control framework.

Key elements of effective fraud prevention include:

- a robust Fraud Policy and Code of Conduct;
- sound fraud risk management processes;
- a comprehensive fraud control plan;
- prudent employee, and third party, due diligence;
- regular fraud awareness training;
- fraud-related controls for activities with a high fraud risk exposure;
- system controls to ensure accurate and up-to-date data; and
- communication about investigation outcomes to demonstrate that allegations and incidences of fraud are serious and appropriately dealt with.

As with other fraud control strategies, an organisation should align the resources it commits to preventative strategies according to the fraud exposure of the organisation.

Figure 5.1 illustrates a range of preventative strategies and measures that an entity could consider to manage its fraud risks. The identified strategies are mapped on a continuum of resource intensity and fraud risk exposure. The preventive measures contained at the base of the triangle generally represent those preventative measures that would need to be implemented by any entity to have an effective fraud control framework. Strategies at the apex of the triangle are more appropriate if an entity has a significant fraud exposure and/or significant resources to introduce the control.

In determining a ‘fit for purpose’ approach to managing fraud risks, the resources devoted to preventative strategies and controls should be proportionate to the fraud risk profile as indicated by, for example, the materiality, scope, complexity, and sensitivity of possible fraudulent activities. The controls identified and their associated costs should be considered with respect to the nature and scale of the fraud risks they are designed to address.
5.1. Fraud risk management

Risk management is crucial to fraud control, guiding the development of an effective fraud control plan and associated strategies and activities to minimise the opportunities for fraud to occur. Risk management provides a framework to identify, analyse, evaluate, and treat fraud risks. While the approach taken may need to be tailored to suit the particular needs of individual entities, using structured and systematic risk management methodologies can assist an organisation to assess the level and nature of its exposure to internal and external fraud threats; establish its fraud risk profile so that appropriate resources can be allocated to mitigate or minimise significant fraud risks; and evaluate the effectiveness of its risk control measures.

Because there is often considerable overlap between organisational risks—that is, enterprise risk, business risk, audit risk, security risk and fraud risk—it is important that fraud risk assessments are considered in the broader context of organisation-wide strategic planning and risk assessment. Figure 5.2 illustrates how organisational risks can overlap. This overlapping of risks means, in turn, that controls addressing these risks may intersect. For example, security controls to manage risks to the integrity of an organisation’s information systems can be equivalent to the fraud controls required in the same systems. In addition, a robust fraud control plan can itself be an effective control in the treatment of an organisation’s reputation and/or business continuity risks.
5.1.1. Fraud risks

A central objective in fraud control is to minimise the risk of fraud occurring. The sources of fraud risk will vary according to an entity’s profile. The following elements will typically assist an entity to determine its fraud risk context:

- role and functions;
- impact of change in structure or function;
- the operating environment and the entity’s relative exposure to external and internal fraud; and
- exposure to ongoing and emerging fraud risks.

5.1.2. Entity role and functions

Entities in the general government sector undertake a variety of roles and functions including: policy development and/or review; procurement, including tendering and managing supplier interfaces; revenue collection and administration of payments to the general public (including social, health, and welfare payments); service delivery to the general public, including through program and contract management; and administration of regulation.

An entity needs to consider the nature of its role and function when identifying its fraud risks and mitigation strategies. For example, an entity that interacts with the broader community is likely to have a different set of fraud risks from one with a policy development focus with little formal contact with the community.
5.1.3. Change in structure or function

Government policy or ‘machinery of government’ changes may require the work performed by particular entities to change, if required by the government of the day. For instance, an entity may be required to introduce a new program, undergo changes to its structure, lose or inherit functions, or change the means of delivery of an existing program. If an entity does undergo a substantial change in structure or function, it should review its fraud risk assessment.

5.1.4. Relative exposure to external and internal fraud

The risk of fraud may be internal (perpetrated by an employee or contractor of an organisation) or external (perpetrated by a customer or an external service provider or third party). In complex fraudulent activity there may be collaboration between employees, contractors and/or external service providers.

Common types of internal fraud include: theft or misuse of tangible assets (cash, inventory, plant and equipment) by employees; theft or misuse of intellectual property or other confidential information (including health, tax and personal records); financial reporting fraud; release or use of misleading information for the purposes of deceiving, misleading or to hide wrongdoing; false invoicing; credit card and other payments fraud; receiving bribes or improper payments; and misuse of position by employees in order to gain some form of financial or non-financial benefit (corruption). Typically, the principal opportunities for internal fraud to occur arise from poor internal controls.

External fraud, on the other hand, is where the threat of fraud comes from outside the organisation, that is, from external parties. Examples of external fraud include: customers deliberately claiming benefits from government programs that they are knowingly not eligible for; external service providers making claims for services that were not provided; and individuals or businesses intentionally evading payment of taxes to government. Cases of complex fraud may involve collaboration between agency employees and external parties.

5.1.5. Exposure to ongoing and emerging fraud risks

Ongoing and emerging fraud risks identified by entities completing the ANAO’s 2009 fraud survey included: unauthorised or inappropriate use of information technology; the unauthorised access and release of information; the forgery or falsification of records; identity fraud; and opportunities for fraud arising from the way in which government conducts business, such as the outsourcing of service delivery to external service providers, the introduction of new policy initiatives and programs, the introduction of internet-based transactions and electronic information exchange.\(^{16}\)

Table 5.1 illustrates particular entity functions and highlights corresponding examples of potential fraud risks.

---

### Table 5.1: Entity role and typical fraud risk

<table>
<thead>
<tr>
<th>Type of entity / function</th>
<th>Examples of fraud exposure / risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy development and/or review</td>
<td>Consultation with a range of stakeholders both inside and outside APS entities is a key, if not essential, input to policy development work. An example of inappropriate behaviour in an organisation with a policy focus is where a Commonwealth employee makes improper use of inside information, or uses their status, power or authority in order to gain or seek to gain a commercial benefit or other advantage.</td>
</tr>
<tr>
<td>Procurement including tendering and managing supplier interfaces</td>
<td>Government purchases include the acquisition of goods, services, and property, including intellectual property. Public officials should not benefit personally from procurement decisions involving expenditure of public money. During any procurement, the community and potential suppliers have a right to expect government representatives to perform their duties in a fair and unbiased way and that the decisions they make will not be affected by self-interest or personal gain.</td>
</tr>
<tr>
<td>Revenue collection and administering payments to the general public</td>
<td>Tax evasion and benefit fraud (including fraud associated with social, health, and welfare payments) is generally characterised by the deliberate provision of incorrect information in order to secure payments or payment amounts for which the recipient is not entitled. Based on knowledge of their customers, and evidence from within their systems or from outside information, ‘customer-facing’ organisations often undertake reviews that examine a recipient’s circumstances where there is a perceived risk of fraud. The aim of such reviews is to detect a deliberate error, omission, misrepresentation or fraud on the part of a customer.</td>
</tr>
<tr>
<td>Service delivery to the general public including program and contract management</td>
<td>Contracting (or outsourcing) is now an integral part of doing business in the public sector and the delivery of many government programs involves contracting with third-party providers. An example of external fraud includes the fraudulent conduct of service providers who charge the Commonwealth for goods or services that are not delivered, or delivered in an incomplete way.</td>
</tr>
<tr>
<td>Exercising regulatory authority</td>
<td>Risks of corruption and misconduct exist in all regulatory authorities. Failure to minimise these risks undermines public confidence in the regulator, resulting in loss of credibility. An example of corrupt and inappropriate behaviour that may occur in a regulatory authority is abuse of power, that is, when an official uses their authority as a regulator to approve compliance with regulatory requirements in exchange for a benefit or advantage.</td>
</tr>
</tbody>
</table>
5.1.6. Fraud risk assessment and management

The Fraud Control Guidelines require entities to conduct a fraud risk assessment at least every two years and, in doing so, to be consistent with the Australian/New Zealand Standard AS/NZ ISO 31000:2009 Risk Management Principles and Guidelines, and Australian Standard AS 8001-2008 Fraud and Corruption Control when developing their risk assessments and fraud control plans. This risk management process is outlined in the Figure 5.3 below.

**Figure 5.3: Risk management process**

- Establishing the context
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment
- Documented risk assessment
- Communication and consultation
- Monitoring and review


Several features of the fraud risk management process illustrated above are worth highlighting.

A robust fraud risk assessment process involves communication and consultation with relevant employees at all levels within an organisation during all stages of the risk management process. This communication should

---

17. Attorney-General’s Department, Commonwealth Fraud Control Guidelines, Canberra, 2011.
address issues relating to the risk itself, its causes, its impact (if known) and the measures taken to treat it. This approach ensures those accountable for implementing the risk management process and stakeholders understand the basis of decision-making, and the reasons why particular actions are required.18

Establish the context involves articulating the organisation’s objectives and the external and internal parameters to be taken into account when managing risk. This process also sets the scope and risk criteria for the remaining process.

Identifying fraud risks requires organisations to consider both internal and external fraud risks including, where relevant to their operations, the potential for international fraud. Organisations can also consider fraud risks that may emerge in the future, for example, fraud risks arising from a change to an IT system or other significant changes in business processes. It is also important that fraud risks are taken into account in the design of a new system or program. Identifying fraud risks at the system and program levels will assist organisations to assess overall organisational risk, and to reflect these risks in their strategic planning objectives.

As fraud entails dishonesty and deception, the identification of fraud risks requires a sceptical mindset and involves asking probing questions such as: How might a fraudster exploit weaknesses in the systems of controls? How could a perpetrator override or circumvent controls? What could a perpetrator do to conceal fraud?

Documenting and assigning ownership of the risks and controls is important. The business area responsible for managing a particular fraud risk should be identified and the timeframe for implementing any remedial action should also be clearly documented in risk management plans. An example of a fraud risk register is provided at Appendix C.

It is also important to monitor and review the fraud risk assessment regularly. The Fraud Control Guidelines require a fraud risk assessment to be performed at least every two years and coincide with a review of the fraud control plan. The Fraud Control Guidelines also require that where an entity undergoes a substantial change in structure or function, or where there is a significant transfer in function (for example, as a result of outsourcing), the entity must undertake another fraud risk assessment in relation to the changed functions.19 The Fraud Control Guidelines note that, where appropriate, a rolling program may be introduced to update the fraud risk assessment more regularly.

An organisation should also actively monitor and review its identified fraud controls. Changes in the effectiveness or applicability of these fraud controls can impact on the organisation’s fraud risk assessment to either increase or decrease fraud risk. An entity’s internal audit area would generally be expected to assess periodically whether the entity’s fraud control framework is appropriate and is operating effectively (including monitoring the outcomes of the fraud control framework). The Audit Committee oversees this process. This role is explored further in Chapter 8.

5.1.7. Preparation of a fraud control plan

A fraud control plan is developed or updated through the fraud risk management process and contains a documented record of all fraud control activities and strategies and their owners. As with the fraud risk assessment, the fraud control plan requires review every two years or earlier if the organisation experiences significant change.

19. Attorney-General’s Department, Commonwealth Fraud Control Guidelines, Canberra, 2011.
The Fraud Control Guidelines outline the key features of an effective fraud control plan, which have been included, and enhanced, in Table 5.2 below.

### Table 5.2: Key features of an effective fraud control plan

<table>
<thead>
<tr>
<th>Key features</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>An outline of the structure of the organisation.</td>
<td>Include reference to specific fraud control structures in this section of the plan.</td>
</tr>
<tr>
<td>A statement of the entity’s attitude, definition and approach to fraud.</td>
<td>This statement should match that included in the entity’s Fraud Policy and be endorsed by the Chief Executive.</td>
</tr>
<tr>
<td>Demonstrated links to an up-to-date risk assessment.</td>
<td>This promotes the link between fraud risk and fraud control. Examples should be provided to demonstrate this.</td>
</tr>
<tr>
<td>Summary of the fraud risks identified.</td>
<td>This promotes awareness among staff of the fraud risks faced by an organisation.</td>
</tr>
<tr>
<td>Outline the key controls in place to address all identified high-rated fraud risks.</td>
<td>Information should be provided on the types and nature of fraud controls to inform employees within the organisation. Where possible links should be made to the organisation’s business planning process.</td>
</tr>
<tr>
<td>Address both internal and external fraud risks.</td>
<td>Employees need to be aware of the existence of internal and external fraud.</td>
</tr>
<tr>
<td>Include a timeline for taking actions on all strategies.</td>
<td>This timeline should include realistic deadlines and include monitoring of the implementation of these strategies and controls.</td>
</tr>
<tr>
<td>Assign ownership for the design, implementation and evaluation of identified fraud controls.</td>
<td>The assignment of ownership is critical in establishing accountability and promoting compliance with the fraud control plan. These responsibilities should also be highlighted in individual performance agreements.</td>
</tr>
<tr>
<td>Reinforce the responsibilities that all employees have for fraud control.</td>
<td>This provides another avenue to remind employees of their responsibilities in relation to fraud control.</td>
</tr>
<tr>
<td>Detail how employees can report and respond to suspected fraud.</td>
<td>This will provide employees with enough information on how, and to whom, they should report suspected instances of fraud.</td>
</tr>
<tr>
<td>Outline how fraud is investigated within the organisation.</td>
<td>Information relating to the investigation process enables employees to understand how fraud is investigated and treated within their organisation.</td>
</tr>
<tr>
<td>Include a summary of relevant awareness-raising and training strategies.</td>
<td>This provides information on the fraud awareness-raising activities that are undertaken.</td>
</tr>
</tbody>
</table>

Chapter 8 provides further guidance on the necessary monitoring and review activities that should be undertaken to ensure that the fraud control plan is current and relevant to the needs of the entity.
5.1.8. Organisation size

The nature and materiality of the internal and external fraud risks faced by small public sector entities could be expected to be different from the fraud risks faced by large ‘client-facing’ entities. For this reason, a better practice principle for small public sector entities is to have ‘fit for purpose’ mechanisms in place to combat fraud.

To mitigate the risk of internal fraud occurring, the control structures within small organisations should have a basic level of preventative controls. For example, avoiding the concentration of key decision areas in the hands of a single individual is fundamental to the prevention of fraud. Although the separation of duties is a powerful internal control, it is not always feasible in small organisations. Accordingly, there should be compensating controls in place such as the Chief Executive or Board approving some transactions.

5.1.9. Outsourcing of fraud control activities

Many entities choose to outsource various aspects of their fraud control arrangements. The Fraud Control Guidelines provide information on the outsourcing of fraud control activities, the key criterion being that the outsourcing does not compromise the entity’s fraud control arrangements. In reaching the decision to outsource aspects of its fraud control arrangements, an entity must ensure the outsourced provider is: suitably qualified and experienced; complies with the requirements of the Fraud Control Guidelines; is familiar with the entity’s internal policies and procedures and applicable legislative responsibilities, as well as any potential conflicts of interest; and committed to complying with the requirements of the Privacy Act 1988.

In addition, it is better practice for an entity outsourcing any or all of its fraud control to ensure:

- a fraud risk assessment is undertaken as part of the development or update of its existing fraud control plan;
- the fraud control plan covers all aspects of the entity, including its programs and services;
- an in-house contact point is assigned for reporting and recording all allegations of fraud; and
- the purchasing entity appoints a manager to be responsible for fraud control overall.

While all or part of the fraud control arrangements can be outsourced, entities remain accountable for meeting their obligations under legislated requirements and the Fraud Control Guidelines.

20. Attorney-General's Department, Commonwealth Fraud Control Guidelines, Canberra, 2011.
**ABC fraud surveys**

The Australian Broadcasting Corporation (ABC) last undertook a comprehensive fraud risk assessment to establish its fraud control plan for 2008–10. The fraud risk assessment was undertaken by an external organisation under oversight and direction from the ABC’s internal audit department. The key challenge for the ABC is to maximise coverage to canvass and assess fraud risks as well as using the fraud risk assessment as a fraud awareness tool, when it:

- is geographically spread throughout Australia and overseas;
- operates and broadcasts on a 24/7 basis; and
- has a workforce that reflects the diversity of all its operations—media, broadcasting, commercial and retail, online, transmission, IT and support.

The fraud risk assessment involved the use of an all-staff survey which was accessible over the internet and was hosted by an external organisation. The survey was launched by the Managing Director and reinforced by periodic ‘pop ups’ when staff logged into the network. It was completed by more than 790 staff and was used to assess risks across a range of processes in the organisation and to collect statistical data by location, division and role while maintaining the confidentiality of individual respondents.

This approach allowed the ABC to generate fraud risk assessments for each division and the Corporation overall. As well as informing the annual audit plan, the statistical information was used by the ABC’s internal audit department to tailor and target fraud awareness activity and information.

### 5.2. Fraud policy

As part of fostering an environment that encourages fraud prevention and control, the Fraud Control Guidelines provide that ‘agencies must prepare and widely distribute a fraud policy statement’.21

A fraud policy statement assists employees to understand what fraud is, their organisation’s attitude to fraud, and what to do if they suspect fraud is being perpetrated. Typically, a fraud policy statement is part of other corporate documentation, such as Chief Executive Instructions.

The key purpose of a fraud policy is to detail what is expected of employees, clients and suppliers and the consequences of engaging in fraudulent conduct. An effective policy on fraud includes:

- the definition of fraud and an outline of the organisation’s position on fraud;
- an assurance that all allegations and investigations will be handled confidentially; and
- directions about how allegations / incidents of fraud are to be managed.

The policy should also outline what employees should do if they suspect the perpetration of fraud (see Chapters 6 and 7 of this Guide).

---

21. Attorney-General’s Department, Commonwealth Fraud Control Guidelines, Canberra, 2011.
5.3. Preventative measures

5.3.1. Code of conduct

A robust code of conduct is integral in establishing an ethical culture. Chapter 3 of this Guide outlines the APS Values and Code of Conduct.

For Australian Government agencies, the APS Values and Code of Conduct are the benchmark statements of appropriate behaviour for public servants. Where applicable, entities can develop a Code of Conduct that suits their needs and that encapsulates issues unique to their organisation. This would need to be consistent with the APS Values and Code of Conduct.

If an entity does not have its own Code of Conduct then it needs to ensure that the APS Code of Conduct is promoted throughout the organisation and forms part of the organisation’s culture. Entities should also consider whether there is adequate consideration of ethical standards in the: induction and ongoing staff training; and performance management of staff.

5.3.2. Conflicts of interest

The management of conflicts of interest is an integral part of establishing an ethical culture. Of primary concern within a government entity is the conflict between private and public interests, and the effective management of this issue.

The Australian Public Service Commissioner provides some practical guidance for agencies on how to actively manage conflicts of interest:

- register or declare in writing a possible or potential conflict of interest to a manager (for an agency head, this will be the relevant Minister);
- restrict involvement of APS employees in matters in which they have (or are perceived to have) a conflict of interest;
- recruit third parties who do not have an interest (such as probity advisers) to advise on or participate in the matter;
- remove APS employees from involvement in matters in which they have real or perceived conflicts of interest;
- an APS employee may have to relinquish assets or other private interests; and
- in rare circumstances, APS employees may need to resign from their employment.

The ANAO Better Practice Guide—Fairness and Transparency in Purchasing Decisions – Probity in Australian Government Procurement, August 2007, also provides practical guidance on identifying and managing conflicts of interest and includes a checklist that can be used to identify any potential personal interests that could cause a conflict of interest.

5.3.3. Employment screening

The screening of employees is an integral part of an organisation’s fraud prevention strategy. Particulars in respect of employment screening are contained within AS 4811-2006 Employment Screening and the Australian Government Protective Security Policy Framework. This standard requires the verification, with the consent of the individual, of the identity, integrity and credentials of an entrusted person.

The standard, AS 4811-2006, states that employee screening should be undertaken in respect of all persons joining an organisation and for all personnel being transferred to a senior executive position, or to a position considered by the organisation to be a higher risk in terms of the potential exposure to fraud or corruption. This approach enables the early identification of changes in risk factors such as lifestyle or financial pressures and enables an organisation to be proactive in managing the risk of fraud. Re-screening of employees should be considered by organisations in the context of the risks represented by their roles and the costs associated with undertaking this activity.

Practical steps to be taken in the screening of a new staff member include:

- verification of identity, including presentation of two different forms of identity documents;
- police criminal history search in all states and any countries where the individual has resided;
- reference checks with the two most recent employers and any public sector employer;
- checking with any relevant professional licensing or registration board to determine whether an inquiry by a professional licensing or registration body is pending. Examples include such organisations as the Institute of Chartered Accountants in Australia, CPA Australia or the relevant State or Territory Bar Association;
- consideration through interview and any necessary follow-up of any employment history gaps and reasons for those gaps; and
- verification of qualifications through an independent source, for example, by calling the relevant institutions rather than relying on information or documentation provided by the individual.

5.3.4. Fraud awareness training

All staff members should have a general awareness of fraud, how they should respond and the organisation’s processes if this type of activity is detected or suspected within their workplace. Fraud awareness training is an effective method of ensuring that all employees are aware of their responsibilities for fraud control and of expectations pertaining to ethical behaviour in the workplace.

Ensuring that employees understand what constitutes fraud and the cost of fraud to the organisation and the Commonwealth as a whole, is another key objective of fraud awareness training. The training of managers and staff can assist them to recognise the common behavioural signs that fraud is occurring, and encourage them not to ignore these ‘red flags’.

27. AS 8001-2008 Fraud and Corruption Control, para 3.7.1, p.38.
It is preferable that fraud awareness training is conducted alongside other related training such as the APS Values and Code of Conduct, the ethical culture of the organisation including any organisation-related policies (such as ‘no unauthorised browsing of client records’), whistleblowing policy and processes including unlawful disclosure of official information and compliance with the Privacy Act 1988.

There are a number of different approaches that can be used by organisations in delivering effective fraud awareness training. The list below outlines a number of approaches which are currently in use in the APS, including:

- distributing cards containing details of the fraud reporting channels;
- providing training on fraud control to all staff;
- printing fraud awareness articles in staff newsletters;
- producing wall posters, pamphlets, brochures, booklets, bookmarks and fact sheets;
- including messages with fortnightly electronic pay slips;
- maintaining specific security and fraud control intranet sites;
- links on entity websites to enable members of the public (including external service providers) to report suspected external fraud;
- publishing an abridged version of the entity’s fraud control plan;
- including information on fraud matters in weekly communications from the Chief Executive to staff;
- using guest speakers to deliver presentations to staff;
- establishing a fraud control officer network; and
- publicising information on fraud prosecutions and outcomes.

The use of these approaches should be considered in the context of the individual organisation to ensure they are ‘fit for purpose’ and that measures are matched to the specific risks and available resources of the particular organisation.

5.3.5. Fraud awareness training strategies

Fraud awareness training provided to new staff members at induction, and periodic refresher courses provided to all staff including management, will assist in ensuring that employees are aware of their responsibilities in relation to fraud control. It is important that all the necessary fraud control information is provided to staff in these forums. A case study undertaken at the New Zealand Inland Revenue Department identified that employees did not generally read the organisation’s Code of Conduct until it was breached. This demonstrates that the mere existence of a robust Code of Conduct is not generally sufficient to make employees aware of their responsibilities.

In addition to setting the organisation’s expectations for ethical behaviour and the potential sanctions for fraudsters, fraud awareness training needs to emphasise the potential benefits and organisational rewards for professional behaviour. For example, Australia Post fraud awareness training has emphasised the increased job
security and organisational profitability associated with good fraud control, and the Australian Federal Police link ethical behaviour to career progression.

A good fraud awareness training regime includes information on:

- the principles of the FMA Act, privacy and confidentiality legislation and awareness, the Public Service Act 1999 and underpinning expectations such as Values and Code of Conduct and ethical standards (including how to report fraud and unethical behaviour) and conflicts of interest policy;
- what constitutes fraudulent conduct, including practical examples of fraud and the potential benefits fraudsters seek to obtain (intangible and tangible);
- how and where to communicate concerns about known or potential wrongdoing;
- responsibilities for the prevention, detection, investigation and reporting of unethical behaviour including the roles of the individual, the Fraud Manager and the Chief Executive;
- the organisational and personal benefits of effective fraud control;
- the signs or ‘red flags’ associated with potentially fraudulent activity;
- whistleblowing mechanisms, protections and consequences for inappropriate disclosures;
- the potential disciplinary consequences for those who engage in unethical behaviour;
- the role of (internal) conduct investigations; and
- the role of the Australian Federal Police and the Commonwealth Director of Public Prosecutions where serious criminal behaviour is alleged.

Consideration should also be given to the design of specific and ongoing refresher fraud training for employees who work in areas in which there is a higher risk of fraud.
Fraud Control–Prevention

Case Study

Customs Z Card

Australian Customs and Border Security have embarked over the last 18 months on the implementation of a comprehensive fraud awareness-raising plan. This involved the presentation of awareness training to over 4000 employees with information concerning:

- what is ethical behaviour and what is required by Customs;
- definitions and examples of criminal and administrative matters;
- the Customs fraud control framework;
- the legislative environment;
- the Code of Conduct;
- whistleblowing provisions and protections;
- the investigative process and sanctions available; and
- case studies of real life examples within Customs.

The awareness program also involved the distribution of the Customs’ Z Card. The Z Card is a credit card-sized document which contains key information including reporting avenues and the fraud control framework. Its size allows the Z Card to be kept by the employee at their desk or in a convenient place, which allows quick referral should the need arise.

5.3.6. Non-government service providers

Service delivery by government is sometimes undertaken by non-government service providers. This does not absolve either organisation of their fraud control obligations. Raising awareness of fraud both committed by and against third-party providers is essential. Organisations providing services to and on behalf of government should be made aware of the Commonwealth’s position regarding fraud and ethics and the organisation’s responsibilities, which can be outlined and measured through performance indicators identified in the service or other relevant contracts or agreements.

When establishing relationships with non-government service providers, entities should consider those elements of the Fraud Control Guidelines, APS Values and Code of Conduct that might apply, and how they will be promoted and compliance monitored. This may include the use of provisions in contracts such as:

- having the highest ethical standards;
- delivering services fairly, effectively, impartially and courteously to the Australian public;
- being sensitive to the diversity of the Australian public; and
- implementing fraud control arrangements that meet the equivalent standards of the Fraud Control Guidelines.

For some programs, non-government service providers operate in a sector where a common set of values and codes of conduct already exist, possibly as part of recognised sector / industry quality assurance arrangements. While the APS Values and Code of Conduct provide the benchmark for the delivery of services by the Australian Government, entities can look to apply appropriate elements of recognised industry codes where these codes provide equivalent service standards, supplemented where necessary.

Thought could be given to reviewing the service provider’s fraud control arrangements, inviting attendance to the purchasing organisation’s fraud awareness training and requiring the service provider’s staff to sign a code of conduct declaration.

5.3.7. Screening service providers

Confirming the identity and reputation of service providers is important in managing fraud control within an organisation. The vetting of service providers should be tailored to the materiality and relative risk the individual or organisation represents.

The standard, AS 8001-2008 Fraud and Corruption Control requires organisations to ‘take steps to ensure the bona fides of new suppliers and customers and periodically confirm the bona fides of continuing suppliers and customers’.31

Depending upon the relative importance and risk presented by the service provider, practical steps an organisation can take to verify their bona fides on both an initial and periodic basis include:

- checking that the organisation’s trading address and telephone listing matches its contact details;
- searching the company register (if the supplier is incorporated);
- confirming that the organisation’s Australian Business Number (ABN) corresponds to its company register ABN;
- verifying the personal details of directors, including conducting a bankruptcy search and disqualification search;
- confirming current legal proceedings pending and judgments entered; and
- confirming the entity’s registration with the appropriate chamber of commerce or industry association (if applicable).

5.3.8. Fraud controls for higher risk processes and activities

Certain processes or activities have a higher fraud exposure than others. These high-risk areas should be analysed to determine whether they need to be the subject of specific fraud controls. It is important that the controls established to manage these high-risk areas are actively monitored and understood by relevant personnel. Examples of processes with a higher inherent fraud risk include: accounts payable; cash handling; pre-payments; travel and subsistence payments; works contracts; and grant programs.

Examples of specific preventative fraud controls that can be applied to one or more identified fraud risks include:

- segregation of duties;
- hard coded IT system controls (that is, access restrictions or dollar value limits for processing transactions);
- effective procedural controls and management oversight where appropriate;
- physical security measures, including the use of safes and physical access restrictions;
- the deterrent effect of regular and random quality assurance checks by management to determine the existence of a service or goods procured;
- regular supplier reviews and the maintenance of a register of non-compliance/breaches of contractual conditions and reporting requirements; and
- rotation of personnel in high-risk positions (requiring staff to take regular annual leave and balances not to accrue to high levels).

5.3.9. Controlling the risk of corruption

With the increased international focus on corruption and the authority exercised by members of the APS, the risk of corruption should be specifically considered by all public sector entities. Transparency International and the Organisation for Economic Cooperation and Development have produced integrity and anti-corruption publications which have informed the Australian Standard AS 8001-2008 *Fraud and Corruption Control*.

An effective anti-corruption program should include:

- strong anti-corruption, anti-bribery provisions;
- a policy of personnel rotation in high-risk positions so that improper relationships are less likely to develop;
- vendor audits of high-risk providers;
- enhanced probity and contracting procedures; and
- multiple open channels of communication with employees, customers, vendors and other third parties to encourage those parties to come forward if they have any concerns relating to corrupt conduct.

5.4. Communication of identified fraud

Awareness of there being a high likelihood of getting caught is an effective deterrent to economic crimes such as fraud, as it demonstrates the risk of obtaining rewards through dishonest behaviour. Providing information to employees and customers on fraud detected and action taken indicates there are consequences attached to committing fraud and this can act as an effective deterrent.

32. Note that some of these controls are also applicable as detective controls.
While an organisation may have a desire to avoid adverse media attention, the public reporting of de-identified information in relation to fraud investigations serves the following purposes because it:

- illustrates contemporary ethical issues and can be used as part of a fraud awareness program;
- acts as a deterrent to others;
- demonstrates that disciplinary decisions are taken against those found guilty of committing fraud; and
- demonstrates the organisation's commitment to having an ethical and anti-fraud culture.

5.5. Building fraud prevention into program design

When considering the features of a new government policy or program, the design characteristics will influence the inherent capacity of the initiative to be delivered with a high level of integrity. Factors that affect the potential for fraudulent activity in a program include the degree of flexibility in the eligibility rules and the schedule of services to be provided. Where the risk of fraud is high, it is appropriate to introduce preventative controls, such as increased requirements for personal and other relevant information to establish eligibility and the appropriate level of payment, in order to reduce the potential for fraud.

5.5.1. Fraud risk assessment

Organisations designing and/or implementing a significant program should prepare a fraud risk assessment to identify, analyse and evaluate the fraud risk inherent in the proposed program. This fraud risk assessment should comply with the Australian and New Zealand standard on risk management, AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines, as outlined earlier in this chapter.

Any fraud risk assessment developed for a program should complement the existing risk management processes and be used to develop an effective anti-fraud program that specifically addresses the fraud risks faced by the program. These measures should be monitored for effectiveness over time, and the fraud risk assessment should not be a one-off exercise.

Fraud risk assessments, at a minimum, should be conducted and/or revised at the following junctures:

- prior to the design / development of the program, in order that the program is designed with minimising or avoiding fraud risks in mind;
- after the program has been developed, but prior to implementation, in order to assess the appropriateness of the design and the adequacy of the proposed controls;
- during the period after implementation of the program, to consider operational practicalities that may not have been envisaged, to consider actual frauds or complaints occurring, and to consider the effectiveness of controls in their actual operation;
- in the event that material changes are made to the design of the program during its operation, to detect new frauds that may be possible as a result of changes to policy or procedure; and
- during the close-out phase of a program to ensure any new fraud risks created by the closure of the program are managed.
Fraud risk assessments conducted on this basis will assist the organisation to mitigate fraud risks and reduce the probability of actual incidents occurring (whether serial or opportunistic) that could cause loss to the organisation.

5.5.2. Fraud control plan

While organisations should already have their own fraud control plan, a separate fraud control plan can be considered for large or high-risk programs, to address the fraud risks specific to the program. In instances where large programs cut across several government entities, the lead entity should take carriage of the fraud risk assessment process and ownership of the fraud control plan.

Factors that may influence the decision to develop a fraud control plan for a particular program may include:

- Are the program mechanics complex (for example, eligibility criteria)?
- Are large sums of money to be distributed / expended under the program?
- Will the program be rolled out nationally?
- Will large sections of the population be potential participants in the program? and
- Is the program planned to operate for a long period of time?

The fraud control plan should be revisited on a regular basis and in line with the fraud risk assessment, to incorporate the impact that changes to the structure of the program may have on the likelihood and consequence of fraud risks occurring.

5.5.3. Communication and awareness

According to the Fraud and Corruption Control Standard, all program staff and other stakeholders should be aware of what constitutes fraud and how they should respond if this type of activity is identified. Management should regularly communicate the types of behaviour that constitute fraudulent practice, the fraud control activities in place to manage these risks (where appropriate), and the consequences for individuals who participate in fraudulent conduct.
### BETTER PRACTICE CHECKLIST

#### Fraud prevention

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has the entity undertaken a comprehensive fraud risk assessment in the previous two years, or following any significant change to the entity if earlier?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In identifying the fraud risks, did the entity consider: the entity’s role, size and function; any change in structure or function; external and internal fraud; new and emerging fraud risks; and the broader organisational risks?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has a fraud control plan been developed to minimise the impact and likelihood of identified risks?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has a fraud policy been issued by the CEO outlining the entity’s position on fraud?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do agreements with non-government service providers consider the applicable elements of the APS Values and Code of Conduct?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the entity ensure that adequate employment screening procedures are implemented?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the entity take steps to ensure the bona fides of new suppliers and customers and periodically confirm these?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the entity ensure that adequate fraud awareness activities and training are conducted within the organisation? This should also include external parties such as suppliers and customers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the entity have a formal process in place for communicating the outcomes of completed fraud investigations?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key points

- Because no system of preventative controls can provide absolute assurance, entities should implement systems aimed at detecting fraud.
- Passive detection measures are controls or activities that do not require the active involvement of management but exist as a means by which fraud is detectable within an organisation.
- Active measures are controls or activities that require the assertive involvement of management and by their nature are designed to detect or assist in detecting fraud within an organisation.
- Fraud detection in programs can include regular supplier reviews, data mining and analysis, and internal and external reporting mechanisms such as hotlines, web-based reporting and internal reporting channels.
All Australian Government entities are susceptible to fraud and no system of preventative controls can provide absolute assurance. As such, entities should implement systems aimed at detecting fraud as soon as possible after it has occurred, in the event that the entity’s preventative systems fail.33

The source of fraudulent activity may be: internal (perpetrated by an employee or contractor of an organisation); external (perpetrated by a customer or an external service provider); or complex (for example, involve collaboration between employees, contractors, and external service providers).

Measures to detect internal, external, and complex fraud fall into two main categories, passive measures and active measures, as illustrated in Table 6.1 below.

### Table 6.1: Passive and active fraud detection measures

<table>
<thead>
<tr>
<th>Passive measures</th>
<th>Active measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include controls or activities that do not require the active and ongoing involvement of management, but exist as a means by which fraud is detectable within an organisation. An example of this is a reporting ‘hotline’ so that employees, customers, clients and the general public can report incidents.</td>
<td>Include controls that require the assertive involvement of management and by their nature are designed to detect or assist in detecting fraud within an organisation. Examples include data mining, targeted audits through hot spot analysis, internal audit, quality assurance and the analysis of management accounting reports.</td>
</tr>
</tbody>
</table>

In determining a ‘fit for purpose’ approach to managing fraud risks, the resources devoted to detective strategies and controls should be proportionate to the fraud risk profile (as indicated by, for example, the materiality, scope, complexity, and sensitivity of possible fraudulent activities). The controls identified and their associated costs should be considered with respect to the nature and scale of the fraud risk(s) they are designed to address.

### 6.1. Passive detection measures

#### 6.1.1. Effective internal controls

Internal controls are an effective detector of fraud. The KPMG Fraud and Misconduct Survey 2010 found that 42 per cent of major frauds were detected through internal controls.34 This analysis is supported in the Australian Institute of Criminology’s Annual Report to Government 2007–08, which reported that the overwhelming majority of incidents were detected through internal controls, audit or investigation.35 Effective internal controls are integral to the construction of an effective fraud control framework.

Examples of detective internal controls include: regular independent reconciliation of accounts; independent confirmation of service delivery where suppliers are paid in advance for services; physical security, for example, security cameras; staff who know their jobs (people who are familiar with their jobs are more likely to be able to identify anomalies); job rotation / mandatory leave; comparisons between budgeted and actual figures and the follow-up of discrepancies; audit trails and system access logs and the regular review of these; exception reporting; quality assurance; surprise audits; and management review.

33. AS 8001-2009 Fraud and Corruption Control, para 4.2.1.
34. KPMG, Fraud and Misconduct Survey 2010, p.12.
The scope and frequency of management review activities will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring.

6.1.2. Mechanisms to report fraud allegations

Allegations made by employees, contractors, and members of the public can often lead to the uncovering of fraud. One way organisations can detect fraud is through encouraging employees, contractors, service providers and, where relevant, members of the public to report their suspicions of fraud.

The KPMG Fraud and Misconduct Survey 2010 reported that notification by an external party, employee or anonymous letter / call accounted for 47 per cent of fraud detections for the largest frauds committed in Australia.36 Internationally, tip-offs also represented 46 per cent of fraud detections made within the government sector.37

6.1.3. Fraud allegations made by employees

Employees should be encouraged to report suspected unethical behaviour and be provided with a visible process to enable them to report this easily. Easily accessed guidance material supports employees to readily identify what incidents should be reported and to whom. Guidance could include, for example, advice on reporting to line managers; reporting to Human Resources, in particular, the area that investigates employee conduct-related matters; reporting to the organisation’s fraud control officer; reporting to internal audit; and reporting to an anonymous hotline (if available).

6.1.4. External parties

Members of the public (including an organisation’s customers, suppliers and other stakeholders) can play a role in reporting suspected fraud. These parties may be aware of fraud occurring within an organisation, or being committed against an organisation by an outside party. The Australian Government Services Fraud Tip-Off Line is an example of a mechanism that provides members of the public with a place to report allegations of fraud against the Pharmaceutical Benefits Scheme, the Child Support Agency, Centrelink, and Medicare Australia.

6.1.5. Tip-off or hotline facilities

A tip-off or hotline facility typically provides a method whereby employees and other parties can communicate concerns about potential fraud. International research identified that organisations with fraud hotlines suffered much smaller fraud losses than organisations without hotlines. These organisations also tended to detect frauds seven months earlier than their counterparts. Generally these hotlines allow for anonymity as employees often fear making reports due to the threat of retaliation from superiors or negative reactions from their peers.38

The following are the key features of a hotline facility.

- A hotline is a single point of contact for staff members (and others) to report information on suspected fraud. It gives people a means of contacting the organisation at minimal personal risk. A hotline arrangement also enables staff to obtain advice and information.

- A hotline facility has the advantage of being perceived as being independent of management. Entities may find it beneficial to outsource the hotline service to a third-party provider.

Fraud Control in Australian Government Entities – Better Practice Guide

Chapter 6

55

Fraud Control–Detection

Case Study

• A hotline facility, while predominantly telephone-based, can also sometimes receive reports via other channels, such as email or mail.

• A well-designed hotline provides access to a trained interviewer, operates 24 hours a day, supports a multilingual capability, provides a phone number that is toll-free, and applies consistent protocols for gathering and recording relevant information.

• Matters reported via the hotline are normally treated confidentially, to the fullest extent possible. It can provide anonymity, though it is a good idea to obtain the complainant’s name or as many supporting details as possible to enable better follow-up of an allegation.

• An organisation can use the data on fraud allegations to analyse trends and address emerging risks.

Depending on the size and type of the entity (for example, policy, procurement, revenue collection / payment administration, service delivery, or regulatory), a range of mechanisms can be used to enable fraud allegations to be reported, including: a telephone line, manned by an appointed delegate; an email or postal address, which allegations could be sent to; an electronic mechanism, for example, a form available on the internet that could be submitted electronically.

An organisation’s website can provide advice to informants about the kind of allegations that could be referred to the organisation, including whether the tip-off concerns a member of staff, a customer, or a business. An organisation’s website can also facilitate reporting in cases where a member of the public may be reluctant to talk via telephone.

Airservices Australia ethics hotline

Airservices Australia has established an ethics hotline to allow employees to confidentially report issues of concern. These may include: breaches of the law; fraud; theft; corruption; and unprofessional behaviour, such as bullying, harassment or discrimination.

Airservices Australia uses independent consultants to ensure confidentiality of reporting.

Information received via the ethics hotline is referred to an Ethics Committee. The Committee consists of the General Counsel, the Manager Security and Crisis Planning, the General Manager People and Change and the General Manager Audit and Assurance. It assesses the report and decides whether an investigation is warranted.

If a criminal allegation is received, the Security and Crisis Planning Group conducts an initial assessment of the allegation. It develops terms of reference which must be signed off by the responsible General Manager.

All investigations are conducted according to Australian Government Investigation Standards. A final report is prepared for the responsible General Manager and the Ethics Committee. A briefing is then prepared for the Airservices Australia Chief Executive Officer with a recommendation on whether the matter should be referred to the Australian Federal Police, the Commonwealth Director of Prosecutions or the Airservices People and Change business group for disciplinary action, which may include termination.
6.1.6. Whistleblowing and public interest disclosures

The Public Service Act 1999 provides protection for an APS employee who makes a whistleblowing report. Whistleblowing refers to the reporting, in the public interest, of information which alleges a breach of the APS Code of Conduct (including fraud) by an employee.\(^{39}\) For those entities under the Public Service Act 1999, the senior executive is also required to establish procedures to manage whistleblowing reports.\(^{40}\)

There are Whistleblower Protection Acts or Public Interest Disclosure Protection Acts in all major jurisdictions. These instruments provide schemes that give special protection to disclosures made in the public interest about unlawful, negligent or improper public sector conduct or danger to public health or safety or the environment.

In addition, the Australian Standard AS 8001-2009 Fraud and Corruption Control requires entities to implement a policy for the active protection of whistleblowers and to ensure that the policy is well communicated and understood by all personnel.

It is good practice for an entity to provide information about whistleblowing in its fraud awareness training, specifically the type of information that attracts whistleblowing protections and the persons to whom the disclosure can be made.

6.2. Active detection measures

Active fraud detection measures are controls or activities that require the assertive involvement of management. These measures can be broadly categorised as:

- monitoring and review activities, focused on employees and customers at risk; and
- data mining and/or data matching.

6.2.1. Monitoring and review activities to detect internal fraud

There are a number of ‘red flags’ or early warning signs of fraud activity which can be used to help profile possible internal perpetrators. These early warning signs are summarised in Table 6.2 below.

Table 6.2: Early warning signs for staff and/or workplaces at risk of fraud*

<table>
<thead>
<tr>
<th>Early warning signs: people</th>
<th>Early warning signs: areas or activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unwillingness to share duties; refusal to take leave.</td>
<td>Financial information reported is inconsistent with key performance indicators.</td>
</tr>
<tr>
<td>Refusal to implement internal controls.</td>
<td>Abnormally high and increasing costs in a specific cost centre function.</td>
</tr>
<tr>
<td>The replacement of existing suppliers upon appointment to a position or unusually close association with a vendor or customer.</td>
<td>Dubious record keeping.</td>
</tr>
</tbody>
</table>

---

39. Section 16 of the Public Service Act 1999 prohibits victimisation of, or discrimination against, an APS employee who makes a whistleblowing report.

40. Regulation 2.4 of the Public Service Regulations 1999 requires that agency heads establish procedures to manage whistleblowing reports. The procedures must meet the minimum requirements, as set out in Regulation 2.4.
Early warning signs: people

<table>
<thead>
<tr>
<th>A lifestyle above apparent financial means; the provision of gifts to other staff members.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to keep records and provide receipts.</td>
</tr>
<tr>
<td>Chronic shortage of cash or seeking salary advances.</td>
</tr>
<tr>
<td>Past legal problems (including minor previous thefts).</td>
</tr>
<tr>
<td>Addiction problems (substance or gambling).</td>
</tr>
</tbody>
</table>

Early warning signs: areas or activities

<table>
<thead>
<tr>
<th>High overheads.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank reconciliations not up to date.</td>
</tr>
<tr>
<td>Inadequate segregation of duties.</td>
</tr>
<tr>
<td>Reconciliations not performed on a regular basis.</td>
</tr>
<tr>
<td>Small cash discrepancies over a period of time.</td>
</tr>
</tbody>
</table>

*Adapted from The Audit Office of NSW – Fraud Control Volume 2 Strategy and Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud and Abuse, 2010 Global Fraud Survey.

### 6.2.2. Analysis of management accounting reports

The analysis of management accounting reports can reveal anomalies which may be indicative of fraud. Monthly actual versus budget comparison reports for individual cost centres, reports comparing expenditure against prior periods and reports highlighting unusual trends in bad or doubtful debts all may reveal areas which should be further investigated.

### 6.2.3. Hot spot analysis

Allegations of unethical behaviour raised through the organisation’s reporting mechanisms (hotlines, reports to management via email and other methods) can be ‘mapped’ to show hot spots of potential fraud throughout the organisation. Multiple allegations about an area or individual potentially highlight an issue of either fraud or control weakness. This can be used to target the activities of internal audit, an investigation team or the fraud control officer.

The ‘risk map’ of an organisation could be developed to identify the positions of officials who, because of the nature of that position, may be especially vulnerable to fraud. For these positions, action to detect irregularities and fraud could focus on:

- regular performance appraisals, mandatory disclosure of interests, assets, hospitality and gifts; and
- close monitoring in relation to existing computer data-mining to draw attention to transactions that appear to depart from established norms.

### 6.2.4. Data mining—post transactional review

Indicators of fraud, misconduct and error can often be found within an organisation’s financial and operational data. The use of data mining / analysis techniques and tools can assist with the identification of such indicators.

The benefits of using data analysis include:

- analysis of suspicious transactions, for example, duplicate payments or claims;
- identification of unusual relationships, for example, employee bank account matches a vendor bank account;
• assessing the effectiveness of internal controls, for example, password sharing, employees remaining on the payroll after termination / resignation;

• identification of irregular trends over periods of time, for example, supplier favouritism; and

• an ability to analyse large volumes of transactions over periods of time rather than relying on sampling techniques.

Generally, there are two types of data mining / analysis: retrospective review and continuous auditing / continuous monitoring (‘CA/CM’).

**Retrospective review** generally entails the extraction of historical data (usually data relating to more than one year) from the organisation’s Enterprise Resource Planning (ERP) systems for analysis on a standalone IT system using data analysis software. Retrospective review tools can vary from a spreadsheet or database to software that is specifically designed for data analysis with pre-programmed tests such as duplicate payments tests, and an ability to create tests as required.

**CA/CM** refers to the collection and analysis of current data on a real or near real-time basis, that is, daily, weekly, monthly. CA is generally considered to provide the internal auditor with information regarding risk and controls while CM is generally considered to be a management monitoring function. CA/CM tools can vary from those which monitor transactions real time (much the same way that banks monitor credit card transactions) to tools which analyse data near real time that is, daily, weekly, monthly. CA/CM may also be performed using the in-built functionality in an organisation’s ERP system.

### 6.2.5. Monitoring and review activities to detect external fraud

As advised in the Fraud Control Guidelines, fraud against the Commonwealth is defined as ‘dishonestly obtaining a benefit, or causing a loss, by deception or other means’. Results of the Australian Institute of Criminology’s 2007–08 Annual Reporting Questionnaire indicate that of the external fraud incidents, the focus of the highest number of activities was on entitlements. This category includes obtaining a Commonwealth payment, for example, a social, health or welfare payment by deceit. It also includes revenue fraud, that is, deliberately avoiding obligations for payment to government, including income, customs or excise taxes.

**Compliance reviews**

Most entities that collect revenue or administer government payments conduct reviews across the various revenue and payment types. Based on previous experience, knowledge of their customers, and evidence from within their systems or from outside information, entities may undertake reviews that examine a recipient’s circumstances where there is a perceived risk of fraud. The aim of such reviews is to detect a deliberate error, omission, misrepresentation or fraud on the part of a customer.

Review activity should be targeted to areas of higher risk, and an entity should pursue the most productive method for undertaking reviews. Data mining / matching is a cost-effective method of supporting reviews, including cross-organisational approaches.

**Data mining and data matching**

Compared with manual or routine record checking, technological advances in data processing allow for efficiencies in locating records and potential fraud. Where relevant information is held by other organisations, data mining / matching provides significant benefits including: uncovering and reducing fraud; encouraging better compliance; and improving the quality of data held on the systems of participating organisations.41

---

Organisations need to be mindful of privacy considerations and implement appropriate processes to ensure that any data mining/matching activities conform to legislative requirements.42

6.2.6. Detecting fraud by external service providers

Contracting (or outsourcing) is now an integral part of doing business in the public sector and the delivery of many government programs involves contracting with private sector providers. External fraud includes the fraudulent conduct of service providers who charge the Commonwealth for goods or services that are not delivered, or delivered in an incomplete way. The Fraud Control Guidelines state that ‘Agencies are responsible for preventing and detecting fraud against the Commonwealth including fraud within those outsourced functions performed by external service providers’.43

Most cases of external service provider fraud are discovered through day-to-day contract management and associated controls. The aim of contract management is to ensure that deliverables are provided to the required standard, within the agreed timeframe, and achieve value for money. A central risk to the success of a contract is the management of external service provider performance, including the potential for fraud, or inappropriate conduct by the external service providers.

The ANAO’s Better Practice Guide, Developing and Managing Contracts, provides the following suggested treatments for managing external service provider performance: establish a shared understanding of the contract and the responsibilities of each party; monitor contractor performance regularly, including deliverables and contract conditions; hold specific performance review meetings; only make payments for satisfactory performance; and ensure proper documentation and recordkeeping to provide the necessary evidence to demonstrate non-compliance or potential fraud.

Specifically, in regard to potential cases of fraud, the Guide suggests possible responses including:

• discussing alleged fraud with the agency’s in-house fraud control unit;
• reviewing the need to end the contract for breaches of conditions or non-performance; and
• seeking relevant advice on possible causes of action to end the contract.44

6.2.7. Partnering with other entities

The sharing of information about risk factors and fraud perpetrators within entities and across the public sector is important in the prevention and detection of fraudulent activity. Liaison with other entities may also help target detection activities and the sharing of better practices.

Any forum which brings together organisations with a similar business profile can be used as an opportunity to discuss fraud risk, prevention, detection and response.

6.2.8. The role of internal audit

Responsibility for managing the risk of fraud, like responsibility for managing all risks, rests with management as part of its ongoing responsibilities. However, internal audit can assist an entity to manage fraud control by advising on the risk of fraud and the design or adequacy on internal controls. It can also assist in detecting fraud by considering fraud risks as part of its audit planning and being alert to indicators that fraud may have occurred.

42. Data matching undertaken with external organisations is governed primarily by The Data-matching Program (Assistance and Tax) Act 1990; and the Privacy Commissioner’s Guidelines for the Use of Data-Matching in Commonwealth Administration. See Office of the Privacy Commissioner, Guidelines for the Use of Data-Matching in Commonwealth Administration, February 1998.

43. Attorney-General’s Department, Commonwealth Fraud Control Guidelines, Canberra, 2011.

44. ANAO Better Practice Guide—Developing and Managing Contracts – Getting the right outcome, paying the right price, Canberra, Canberra, 2007.
Audit teams may discover instances of fraudulent activity in the course of conducting internal audits. Internationally, internal audit has been responsible for detecting 15 per cent of all frauds identified in the government sector.\textsuperscript{45} In instances where fraud is detected, it is essential that the matter be reported to the appropriate party, as noted above.

### 6.3. Building fraud detection into program management

Fraud detection is a component of the implementation or delivery phases of government programs. Detection strategies can include:

- regular supplier reviews (including surprise audits);
- retrospective reviews using data mining and analysis;
- continuous auditing or continuous monitoring; and
- internal and external reporting mechanisms (hotlines, website and internal reporting channels).

Because some programs can be short-lived, such as those designed to respond to an economic downturn or a natural disaster, continuous auditing or continuous monitoring will be a more effective detection strategy than retrospective reviews.

Employees play a significant role in the detection of fraud. Without specific fraud awareness training, employees may not be able to identify the early warning signs of fraud in a program and will not be equipped to respond appropriately.

Fraud awareness also extends to participants in the program and an awareness campaign should specifically refer to an organisation’s zero tolerance to fraud, how fraud can be reported and how the organisation will respond to allegations. To obtain information from external stakeholders it is also important that the organisation consider, should the program be sufficiently significant, establishing a complaints or reporting hotline where fraud or misconduct can be reported.

### BEFTER PRACTICE CHECKLIST

**Fraud detection**

| Does the entity have a range of internal and external reporting mechanisms in place for parties to report suspected unethical behaviour (including fraud)? |
| Are the entity’s reporting mechanisms easily accessible by internal and external parties? |
| Does the entity use internal audit to actively review its detective control environment? |
| Does the entity provide sufficient information to enable employees to recognise the possible ‘red flags’ or early warning signs of fraud activity? |
| Does the entity require active fraud detection measures such as data mining or ‘hot spot analysis’? |

\textsuperscript{45}. Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud and Abuse, 2010 Global Fraud Survey, p.19.
Key points

- Fraud investigation and response are key elements of the overall fraud control framework and provide stakeholders with reasonable assurance that perpetrators of fraudulent acts are identified, and appropriate remedies are consistently applied.

- All Australian Government entities that are required to comply with the Fraud Control Guidelines must also comply with the minimum standards for investigations set out in the Australian Government Investigations Standards.

- Under the Fraud Control Guidelines, relevant entities are required to investigate minor and routine instances of fraud, irrespective of whether the outcome of the investigation results in an administrative remedy or is referred for prosecution consideration. Matters involving serious and complex fraud must be referred to the Australian Federal Police.

- Prosecutions are important in deterring future instances of fraud and in educating the public generally about the seriousness of fraud.

- Entities should be committed to recovering financial losses caused by fraud through proceeds of crime and civil recovery processes or administrative remedies.
Fraud response is a key element of the overall fraud control framework. Fraud response strategies provide Australian Government entities and external stakeholders with reasonable assurance that perpetrators of fraud are identified, and appropriate remedies applied.

The investigation of, and response to, fraud involves complex interventions and the adherence to relevant legislation and standards including the: Fraud Control Guidelines; the Australian Government Investigations Standards (AGIS); Prosecution Policy of the Commonwealth; Freedom of Information Act 1982; Crimes Act 1914; Privacy Act 1988; and Public Service Act 1999.

7.1. Fraud investigation

The purpose of a fraud investigation is to gather evidence relating to a specific fraud allegation(s) to determine the facts relating to the matter and to assist in deciding what, if any, action should be taken in relation to the matter(s). Under the Fraud Control Guidelines, relevant entities are required to investigate routine or minor instances of fraud against entity programs and to document the reasons for their decisions, irrespective of whether the initial assessment results in the matter being referred for a criminal investigation. ‘Routine or minor’ is defined as instances of fraud that, on an initial assessment by the entity, would be unlikely to be accepted by the Australian Federal Police (AFP) under its Case Categorisation and Prioritisation Model (see section 7.1.1).

Because the investigation process must give due consideration to a broad range of legislative, policy and practical considerations, such as sufficient evidence to support the prosecution of a criminal charge in a court of law, relevant entities must have regard to the Fraud Control Guidelines and the AGIS, which provide guidance on appropriate investigation competency standards for Commonwealth employees and investigation service providers.

7.1.1. AFP referrals and assistance

The Fraud Control Guidelines stipulate that the AFP has primary responsibility for investigating serious or complex fraud against the Commonwealth. Relevant entities must refer all instances of potential serious or complex fraud offences to the AFP in accordance with the AGIS and AFP referral process published on the AFP’s website. The AFP will review the referral in line with the AFP Case Categorisation and Prioritisation Model and may subsequently undertake an investigation into the matter, or reject the referral, undertake a joint investigation with the entity.

Under the Fraud Control Guidelines, relevant entities that have the capacity and the appropriate skills and resources needed to investigate criminal matters and meet the requirements of the Commonwealth Director of Public Prosecutions (CDPP) in gathering evidence and preparing briefs of evidence are authorised to investigate serious or complex offences against the Commonwealth.

Entities can request AFP assistance or advice in relation to an investigation being conducted by that entity into a suspected fraud matter. The AFP can assist entities with the conduct of search warrants, and can provide the following services to support an investigation:

- forensic services;
- document examination;
- fingerprint analysis;
- DNA;

Under the Fraud Control Guidelines, relevant entities that have the capacity and the appropriate skills and resources needed to investigate criminal matters and meet the requirements of the Commonwealth Director of Public Prosecutions (CDPP) in gathering evidence and preparing briefs of evidence are authorised to investigate serious or complex offences against the Commonwealth.

7.1.2. Australian Government Investigations Standards

All Australian Government entities that are required to comply with the Fraud Control Guidelines must also comply with the minimum standards for investigations set out in the Australian Government Investigations Standards (AGIS). The AGIS establishes the minimum standards for relevant Australian government entities when they conduct investigations. Should the AGIS be in conflict with legislation, the legislative requirement prevails.

An investigation is a project seeking information relevant to an alleged, apparent or potential breach of the law. The primary purpose of an investigation is to gather admissible evidence for any subsequent action, whether under criminal, civil penalty, civil, disciplinary or administrative sanctions. Investigations can also result in disruption or prevention action being taken by entities.

The AGIS is applicable to investigations where an entity determines there are reasonable grounds to suspect non-compliance, involve a conflict of interest or if the seriousness or complexity of the matter requires application of these standards. The term ‘investigation’ can also include intelligence processes which directly support the gathering of admissible evidence. The AGIS applies to all stages of an investigation.

According to the AGIS, the outcome of an investigation does not distinguish between administrative, criminal or civil action and is not a factor in determining the quality of the investigation. Rather, what is important are the standards applied during an investigation and the capacity of the investigative process to withstand administrative, operational and judicial review.

Relevant entities are required to comply with the AGIS to achieve a uniformly high standard of investigation by:

- having up-to-date policies and procedures relevant to their functions and programs and an investigation management system, and file management and activity recording procedures in place;
- complying with the AGIS definition of an investigation and the related primary purpose for gathering admissible evidence for subsequent action;
- documenting their policies and procedures for handling all aspects of the investigation process consistent with the AGIS, from initial consideration of an allegation through to successful prosecution of fraudulent crime and recovery of criminal proceeds; and
- clearly identifying the different investigation methodologies for administrative and criminal investigations and the decision-making in relation to the transition from regulatory / compliance functions to criminal investigation.

47. At the time that this Better Practice Guide—Fraud Control in Australian Government Entities—was being prepared and published by the ANAO, the AGIS was being updated to reflect experience since it was issued in 2003. While the references to investigation standards in this Better Practice Guide reflect the essence of the revised AGIS, the Australian Federal Police (AFP) plans to provide the revised AGIS on-line and, if appropriate, to modify the standards from time to time. Given the specialised nature of fraud investigations, entities should consult the AFP’s website to ensure the currency of their overall approach to the investigation of fraud and to inform their investigation activities.
7.1.3. Identification of fraudulent behaviour

The Fraud Control Guidelines require relevant entities to have information systems in place, appropriate for the number and complexity of investigations undertaken, in order to manage information gathered about fraud. This not only supports sound decision-making at the management level, but also helps entities to identify and address any systemic issues that are relevant to fraud.

It is good practice for an organisation to record every allegation of fraudulent conduct that is reported to it, preferably in a central database. This enables proactive analysis of potential fraud hot spots and it can be used to direct the activities of internal audit. A central database also enables trends and analysis of fraud types to be undertaken and profiles to be developed based on systemic types of fraud cases.

According to the Australian Standard AS 8001-2008 Fraud and Corruption Control, a fraud incident register should include:

- date and time of report;
- date and time of incident detection;
- how the incident was reported to management (anonymous report, line management etc);
- nature of the incident;
- value of the loss to the entity (if any); and
- action taken following detection.

Such a register can be used to facilitate an organisation’s policy for the reporting, analysis and escalation of all detected incidences of fraud and corruption. This policy should be clear on the actions to be undertaken following the reporting of an incident.

**FaHCSIA fraud response governance model**

The Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA) recently established a working group between its Fraud and Compliance Branch and People Branch. The working group meets on a weekly basis to discuss allegations of ‘unethical conduct’, particularly in relation to fraud matters. The working group aims to ensure that all allegations are investigated by the most appropriate party within FaHCSIA to enable the best outcome for the department.

The working group also allows the two branches to identify and discuss potential hot spots and analyse trends with a view to improving education and awareness-raising for employees in the department. The two branches have also developed a complementary suite of reports in relation to matters that are considered by FaHCSIA’s Compliance and Integrity Committee.
7.1.4. Preliminary case assessment of an allegation of fraud

The AGIS outlines the standards required of relevant entities when receiving and dealing with an allegation of fraud and all investigations are to be conducted in accordance with the AGIS. Upon receiving an allegation of fraudulent conduct, a relevant entity needs to consider what should be the appropriate response.

Under the AGIS, a relevant entity must have a procedure covering the initial consideration of a fraud allegation that includes:

- recording of the allegation in an appropriately secure fraud incident register, file and/or electronic case management system, consistent with the Australian Government Protective Security Policy Framework;
- the person responsible for making the initial assessment (the decision-maker) is appropriately trained, as required by the Fraud Control Guidelines, and the entity provides an appropriate level of managerial oversight of decision-making;
- timeframes for initial consideration of the allegation;
- the obtaining of any readily accessible evidentiary information from within the entity, where the collection of such evidence would not jeopardise any future investigation, to allow an informed decision on the type of further action required; and
- the need to document the reasons for the decision and what action is intended. The decision as to how to respond to an allegation of fraud is considered to be a ‘critical decision’ in the fraud investigation process and one which needs to be appropriately documented.48

An entity may also make use of a Case Categorisation and Prioritisation Model (CCPM). This tool aids the decision-maker in making the initial assessment and helps drive transparency and consistency in decision-making. The AFP utilises a CCPM for matters referred from other organisations, and entities can consider adapting the principles in this model for their own decision-making purposes.

As provided under the AGIS, it may be that a preliminary inquiry, or ‘case assessment’, is required before a decision can be made as to how to proceed with the allegation. An initial case assessment is aimed at gaining sufficient information to be able to determine the subsequent appropriate action and could include: an interview of the complainant; some level of financial analysis to identify the potential veracity of the allegation; and such other preliminary steps as necessary to enable the decision to be made.

Relevant entities should ensure that in undertaking any preliminary inquiry, they comply with the AGIS and any entity direction or protocols relating to the handling of allegations of fraud, including those relating to the use of coercive powers to collect evidence. Agencies need to provide clear guidance to their investigators about the use of coercive powers particularly once fraudulent behaviour is suspected and the investigation becomes a criminal investigation.

It should also be noted that, irrespective of whether the decision is made to undertake a criminal or disciplinary investigation, the AGIS standards of investigation must be maintained to allow for the possibility of the allegation becoming more appropriate for criminal investigation. As such, relevant entities must have regard to the Fraud Control Guidelines and the AGIS, which provide guidance on appropriate investigation competency standards for Commonwealth employees and investigation service providers (see section 7.1.6).

7.1.5. Conducting an investigation

Fraud investigations are conducted to determine the facts relating to specific allegations of fraud, through the collection and examination of evidence. The AGIS provides guidance and better practice investigation and case management standards for all investigations. Relevant entities must have in place processes and procedures that are consistent with, or exceed, the model procedures outlined in the AGIS modules.49

For example, relevant entities must have written procedures regarding:

• the process for taking witness statements and conducting interviews with suspects;
• the handling of all physical evidence, including property seizure records, and the storage and disposal of exhibits (there should also be written procedures addressing the audit of the exhibit register as required by the Australian Government Protective Security Policy Framework);
• the conduct of surveillance, including physical and electronic;
• the management of human information sources (also referred to as informants); and
• the use of legislated powers such as the power of arrest, detention, coercion, search warrant execution, production orders and inspection orders.

Investigators must have knowledge of and the ability to apply the principles and elements of their entity’s standards and written procedures.

A fraud investigation and response decision-making process is represented at Figure 7.1. This decision tree has been developed to provide an explanation of, and guidance through, the fraud investigation and response process.

This diagram should not be used as a substitute for the AGIS but rather as a guide to better understand the critical decisions that need to be made and documented, from the initial assessment of the allegation and throughout the fraud investigation and response process.

Outsourcing investigations

In some instances, relevant entities will not be sufficiently resourced to conduct an internal investigative response to allegations of fraud. The establishment of an internal fraud investigations team can be costly and takes time to implement effectively. This will not be an issue for the larger program delivery and customer service entities, but for smaller entities (or entities which traditionally focus on policy development), the most cost-effective option will be to engage external investigations services.

In outsourcing investigation activities, relevant entities must take into account the Fraud Control Guidelines and the AGIS, which provide guidance on appropriate investigation competency standards for investigation service providers (see section 7.1.6). It is also beneficial if providers have demonstrated experience in conducting fraud investigations in an Australian government context, and are sufficiently familiar with the requirements of the Fraud Control Guidelines and the AGIS.

Notwithstanding an entity’s resource constraints with respect to internal fraud response capabilities, all serious and complex fraud matters should be referred to the AFP in the first instance. In addition, a relevant entity must consider whether it may still require support from the AFP in the form of assistance to execute search warrants or in the provision of forensic services (see section 7.1.1).

Figure 7.1: Fraud investigation and response decision tree

**IDENTIFICATION**
- Identification of unethical behaviour (fraud/misconduct/corruption) is made and recorded in entity database

**INVESTIGATION**
- Entity should give consideration to the severity of the following characteristics of the case:
  1. Whether it involves a serious breach of federal legislation
  2. The incident type and impact on Australian society
  3. Whether it requires the execution of a search warrant or implementation of surveillance
  4. Whether for any other reason the entity considers it appropriate to refer the case to the AFP (e.g. Political sensitivity or identity of the alleged offender)

Investigation must comply with Australian Government Investigation Standards (AGIS)

**RESPONSE**
- Decision criteria:
  1. Is there a prima facie case for prosecution?
  2. Is there reasonable prospect of a criminal conviction being secured (i.e. evidence beyond reasonable doubt)

Example decision criteria:
  1. Seriousness of alleged offence
  2. Mitigating circumstances
  3. Youth, age, intelligence, physical health, mental health of alleged offender
  4. Alleged offenders antecedents and background
  5. Passage of time since alleged offence
  See Prosecution Policy for further examples

**RESOLUTION**
- What allowed the fraud to occur?
  - A weakness in controls
  - One-off act by a person in a position of privilege
  - Collusion

Source: KPMG.
7.1.6. Training requirements

In deciding to undertake a fraud investigation, relevant entities must have regard to the Fraud Control Guidelines and the AGIS, which provide guidance on appropriate investigation competency standards for Commonwealth employees and investigation service providers.

The Public Services Training Package PSP04 offers the following qualifications relevant to fraud investigations:

- a Certificate IV in Government (Investigation) for employees or contractors primarily engaged in the investigation of fraud; and
- a Diploma of Government (Investigation) for employees contractors primarily engaged in the coordination and conduct of fraud control investigations.

In addition to appropriate qualifications, a robust internal investigations team should have a good mix of skills and experience. Depending on the needs of the entity an investigations team could include: ex-law enforcement officers; lawyers; intelligence operatives; forensic accountants; Information Technology experts, and subject matter experts for the types of programs and services delivered by the entity (for example, building surveyors, engineers or social workers).

7.2. Responding effectively to fraud

7.2.1. Criminal prosecution

The Fraud Control Guidelines require relevant entities to consider criminal prosecution in appropriate circumstances. The Australian Government’s policy in relation to prosecution of criminal offences is set out in the Prosecution Policy of the Commonwealth, which is available from the CDPP. Prosecutions are important in deterring future instances of fraud and in educating the public generally about the seriousness of fraud.

One of the key questions to be considered in the course of an investigation is whether there is a prima facie case for prosecution. That is, is the evidence sufficient to prove the allegation of fraud beyond reasonable doubt? Briefs of evidence should be prepared in accordance with the Guidelines for Dealings between Commonwealth Investigators and the Commonwealth Director of Public Prosecutions.

Relevant entities may refer cases of suspected fraud to the CDPP by forwarding a brief of evidence. The brief will be examined to decide whether a prosecution should be instituted and, if so, on what charge or charges.\(^{50}\) The Prosecution Policy of the Commonwealth underpins all of the decisions made by the CDPP with regards to prosecuting matters on behalf of the Commonwealth, and is designed to promote consistency in decision-making. This policy also provides the CDPP with discretion to prosecute or not to prosecute, while seeking to meet standards of fairness, openness, consistency, accountability and efficiency in prosecuting offences and in maintaining public confidence.

The Prosecution Policy of the Commonwealth guidelines for decision-making state that:

> A prosecution should not be instituted or continued unless there is admissible, substantial and reliable evidence that a criminal offence known to the law has been committed by the alleged offender.\(^{51}\)

---

\(^{50}\) Commonwealth Director of Public Prosecutions, Prosecution Policy of the Commonwealth, CDPP, Canberra, 2008, Section 3.4, p.11.

\(^{51}\) Commonwealth Director of Public Prosecutions, Prosecution Policy of the Commonwealth, CDPP, Canberra, 2008.
In addition to the evidentiary requirements for prosecution, the CDPP has the discretion to consider whether it is in the public interest to prosecute the offender(s). The factors to be considered in assessing whether it is in the public interest to proceed with a prosecution will vary from case to case, but may include:

- whether the offence has been determined to be serious or trivial in nature based on the entity’s case selection and prioritisation policies;
- any mitigating or aggravating circumstances;
- the age, intelligence, health or any special infirmity of the alleged offender, any witness or victim;
- the alleged offender’s antecedents;
- the staleness of the offence;
- the degree of culpability of the alleged offender;
- the availability and efficacy of any alternatives to prosecution;
- the likely outcome in the event of a finding of guilt; and
- the need for deterrence.

Should there be insufficient evidence to prove an offence to the required criminal standard (beyond reasonable doubt) or there is sufficient evidence for prosecution but the entity concerned considers that the public interest does not require prosecution, the CDPP should still be consulted in any matter which involves alleged offences of particular seriousness. The CDPP should also be consulted whenever the entity has any doubt about what course of action is most appropriate in the public interest.

7.2.2. Civil and administrative remedies

There are numerous civil and equity law remedies and administrative processes available to an entity to deal with people who engage in unethical or unlawful behaviour (be it fraud or misconduct). Entities should obtain advice from in-house or consulting legal professionals as to the remedies available. Entities need to have their own clear policies on the appropriate remedies and the situations in which these remedies will be sought. These include: breach of contract; breach of fiduciary duty; letter of demand for repayment; and breach of the Privacy Act 1988 in relation to information theft.

For internal fraud, an entity may take administrative action under the Public Service Act 1999. Remedies available include, but are not limited to: reprimand; suspension; transfer / reassignment of duties; demotion; termination; penalty; financial recovery; counselling; loss of privileges, and greater scrutiny / increased controls.

7.2.3. Recovery

Once an investigation is complete an entity should consider recovery action. This may be in consultation with the AFP or CDPP if criminal charges are pending.

The Fraud Control Guidelines require relevant entities to be committed to recovering financial losses caused by fraudulent activity through proceeds of crime and civil recovery processes or administrative remedies.

---

The Guidelines also require relevant entities to institute a general policy that recovery action be undertaken where the likely benefit will exceed the recovery costs. In this context, ‘benefit’ is not simply financial, but should include consideration of deterrent value and other non-financial benefits such as public perception and integrity of entity reputation.

Entities should not underestimate the deterrence value of loss recovery. This is particularly important given that fraudulent activity is considered to be an economic crime generally involving the weighing of potential benefits against the risk of discovery and subsequent consequences.\textsuperscript{54} While recovering losses may in some cases cost more than the value of the loss recovered, the value of reducing the potential benefit to fraudsters and its deterrent effect must be considered.

Entities have several options for the recovery of losses, including:

- by agreement through withholding final pay or termination benefits via payroll;
- through civil procedures such as a demand for payment or similar, pursued via the courts if necessary (bankruptcy law can be used to recover losses where the individual has insufficient cash assets);
- criminally—through a restitution order flowing from a criminal conviction; or
- under the \textit{Proceeds of Crime Act 2002} (the Act provides a scheme to trace, restrain and confiscate the proceeds of crime against Commonwealth Law).

\section*{7.3. Fraud response in program delivery}

A timely and effective response to external fraud in government programs is critical in sending a strong message to program participants and/or recipients that fraudulent and dishonest behaviour will not be tolerated. This deterrence effect can benefit other government programs and services, as many individuals and businesses can be participants and recipients in other government programs.

Because some programs involve initiatives across organisations, it is important that fraud control activities, including fraud response, are effectively coordinated across entities. In addition, the Fraud Control Guidelines specify where an investigation discloses criminal activity involving another entity’s activities or programs, the investigating organisation must report the matter to that entity, subject to any requirements or limitations under the \textit{Privacy Act 1988}, the Information Privacy Principles or entity legislation regulating the disclosure of information.

Department of Climate Change and Energy Efficiency fraud response

In February 2010 responsibility for closure and finalisation of the Home Insulation Program was transferred to the Department of Climate Change and Energy Efficiency (DCCEE). One of the key priorities for DCCEE was the initiation of a robust response to the suspected cases of fraud in the program. A first step in this response required a post-closure fraud and non-compliance strategy, which included the identification of fraudulent activity such as claiming for insulation installations which had not been undertaken.

DCCEE engaged external forensic services to identify installers who had potentially demonstrated serious non-compliant behaviour. In accordance with the fraud and non-compliance strategy these installers were then subject to a response which was proportionate to the degree of suspected non-compliance or fraud. The types of responses included fraud investigation, civil debt recovery and referral to state and territory regulatory authorities.

Another key component of DCCEE’s response was the creation of an Investigations and Intelligence Branch with responsibility for investigating instances of serious fraud identified in the program. The branch was supported by best practice standards and procedures conforming with the requirements of the Fraud Control Guidelines and AGIS. In addition, DCCEE negotiated a Joint Agency Agreement with the AFP which included the out-posting of a dedicated officer to assist the department in referring serious and/or complex matters to the AFP, and facilitating the conduct of joint entity investigations for less serious matters.

BETTER PRACTICE CHECKLIST

Fraud response

- Is there a system (fraud incident register) for recording allegations?
- Are employees or contractors responsible for conducting investigations on behalf of the entity appropriately qualified?
- Does the entity use the Australian Government Investigations Standards when conducting investigations?
- Does the entity use a Case Categorisation and Prioritisation Model to aid in the preliminary assessment of fraud allegations?
- Is there a general policy that recovery action be undertaken where the likely benefit will exceed the recovery costs?
- Are there processes in place in relation to seeking recoveries?
Key points

- Assessing the performance of fraud control activities is an important element of an entity’s accountability to key stakeholders, such as the Portfolio Minister, the Attorney-General, clients, the Parliament and the general public.

- Fraud control plans should be subject to regular monitoring and revision, to ensure fraud controls are implemented effectively and achieving their intended outcomes.

- The reporting of fraud control outcomes can provide a deterrent effect which will assist an entity in minimising the impact of fraud on its operations.

- Evaluations of an entity’s fraud outcomes can assist managers to assess the continued relevance and priority of fraud strategies in light of current and emerging risks, and ascertain whether there are more cost-effective ways of combating fraud.
An effective fraud monitoring, evaluation and reporting regime provides assurance that legislative responsibilities are being met. It also promotes accountability in responsible areas within entities by providing information that demonstrates their contribution towards compliance and in achieving entity-specific fraud control strategies. Assessing the performance of fraud control activities is an important element of an entity’s accountability to key stakeholders, such as the Portfolio Minister, the Attorney-General, clients, the Parliament and the general public.

The ANAO’s audit of key aspects of Australian fraud control arrangements in Australian Government entities concluded that while there had been an improvement in the level of compliance with the Fraud Control Guidelines between 2002 and 2009, a key area for improvement was the evaluation of specific fraud control strategies.

### 8.1. Monitoring and evaluation

Effective monitoring and evaluation of an entity’s fraud control strategies can assist managers and other decision-makers to: assess the continued relevance and priority of fraud strategies in the light of current and emerging risks; test whether fraud strategies are targeting the desired population; and ascertain whether there are more cost-effective ways of combating fraud.

Evaluations also have the capacity to establish causal links and, over time, an evaluation strategy has the potential to provide insights into:

- the appropriate balance between fraud prevention and detection strategies; and
- the relative weighting of entity incentives that focus on reducing the potential losses from fraud in the first instance, as opposed to discovering fraud after it has occurred.

Analysis can also be undertaken on the effectiveness of established controls through undertaking a cost / benefit analysis both pre and post-implementation of fraud controls. This can often demonstrate savings made by an entity where effective fraud controls have been implemented.

#### 8.1.1. Fraud risk assessment

As outlined in Chapter 5, an entity’s fraud risk assessment(s) needs to be updated at least every two years or in the event of a significant change occurring within an entity. An effective monitoring and evaluation regime needs to be established to ensure that the significant fraud risks of the entity are being accurately captured and recorded.

#### 8.1.2. Fraud control plan

An effective fraud control plan should also be subject to regular monitoring and evaluation, which should seek to answer the following two questions: ‘Is it up to date’ and ‘Is it effective’?

**Is it up to date?**

The fraud control plan should be updated regularly to ensure that the individuals tasked with activities under the fraud control plan are still the individuals in those key positions. Significant changes should trigger an update of the entity’s fraud control plan to ensure it contains accurate and up-to-date information. As outlined in Chapter 5, a fraud control plan should be updated at least every two years, or sooner if the entity experiences significant change.

---

Is it effective?

Changes including new technologies, changes in organisational operations and the commencement of new initiatives can render existing fraud controls ineffective or inappropriate. An entity should review its fraud control plan to ensure it is implemented appropriately and that it remains relevant to the risks being faced.

Testing the effectiveness of a fraud control plan could include:

- ensuring risk assessments have been undertaken appropriately;
- awareness-raising and training are evaluated and are shown to work well in practice;
- allegations are recorded, analysed and followed-up in a timely fashion;
- cases of fraud are dealt with according to applicable external and internal standards;
- remedies are applied appropriately;
- information on cases of fraud are used to update the fraud risk assessment and strengthen controls; and
- that accurate information is provided to the Audit Committee on a timely basis.

It is appropriate to evaluate the controls identified in a fraud control plan to ensure they are implemented and achieving the intended outcomes. If the controls seek to minimise significant fraud risks, consideration should be given to the frequency of the evaluations. Any such review should test the effectiveness of control design and operation and, if possible, seek to benchmark the entity’s fraud performance (and hence the effectiveness of its controls) against other entities.

The following are examples of benchmarks that might be used for evaluating the effectiveness of the response elements of an entity’s fraud control arrangements:

- the timeframes within which allegations of fraud are investigated and fact-finding is completed;
- the percentage of fraud investigations that are completed within the timeframes required by AGIS and internal requirements;
- referrals accepted by the CDPP;
- requests by the CDPP for additional evidence to support the alleged criminal offence; and
- referrals accepted by the CDPP that are successfully prosecuted (includes convictions that are not recorded).

8.1.3. Evaluation of individual fraud cases

Evaluation is the final element in consolidating an entity’s fraud control activities. After any incidence of fraud, whether or not an offence is proven in a court of law, an entity should investigate the situation which allowed the fraud to occur to determine whether it is a result of:

- a one-off action by a person in a position of privilege (any new person in this position may be subjected to additional or periodical screening or monitoring);
- the inadequacy of internal controls (in this case the controls should be re-evaluated and any deficiencies remedied), or;
- collusion (internal control systems can often be overridden by two or more people acting in conjunction with one another).
Evaluation activities can be coordinated by a Fraud Manager so that identified deficiencies and/or recommendations can be applied consistently to similar programs/processes. The outcomes of any hot spot analysis should also be taken into consideration.

8.1.4. Measuring the loss of fraud

Many organisations are now maintaining accurate records of losses due to fraud or are embarking upon forensic audits using statistical sampling and actuarial techniques to measure the cost of fraud. The identified fraud is then analysed to identify the fraud types and the root causes of the problems, for example, internal control weaknesses / breaches, poorly designed application forms or processing errors. This analysis will generally involve a review of source documents and data and may also include interviews with staff and third parties.

These results provide an organisation with the ability to perform a cost / benefit analysis of the implementation of additional controls to either prevent or detect the types of fraud occurring. The assessed savings can then be confirmed in a re-measurement of fraud losses in subsequent periods following the implementation of the improvements.

8.2. Reporting

For a fraud control framework to be effectively implemented, both internal and external stakeholders need to be aware of the outcomes of the fraud control activities undertaken. The reporting of these outcomes can also provide a deterrent effect which will assist an entity in minimising the impact of fraud on its operations. Timely, accurate and up-to-date data is critical in this process.

8.2.1. Internal reporting

Effective internal reporting channels are critical to the management of fraud risks within an entity. Central to this is the role of a Fraud Manager, who establishes and manages these information channels so that the right level and content of information is reported to the right audiences.

The head of an entity’s internal audit area should report to the entity’s Chief Executive / Board and Audit Committee on the outcomes of any monitoring and evaluation activities as well as any investigations and/or outcomes of prosecutions or civil action. To assist priority-setting, an entity can set reporting thresholds for the reporting of individual cases of fraud to the Chief Executive / Board and Audit Committee. A useful strategy is to report fraud trends over time including changes to the level of fraud within an entity by type, for example, trends in the inappropriate use of information, travel fraud and identity fraud.

8.2.2. External reporting

FMA Act agencies are required to report on fraud matters to their Portfolio Minister and annually to the Minister for Justice and Customs. FMA Act agencies are also required to certify in their Annual Report to Parliament that they comply with the Fraud Control Guidelines.

Information to be included about fraud control in Annual Reports to Parliament are set out in ‘The Requirements for Annual Reports for Departments, Executive Agencies and FMA Act Bodies’, which is prepared by the Department of the Prime Minister and Cabinet and approved by the Joint Committee of Public Accounts and Audit.
Since 2006–07, the Australian Institute of Criminology has annually collected fraud statistics for the Commonwealth. Entities are required to answer a questionnaire and this information is consolidated and included in the Commonwealth Fraud Control Annual Report to Government. The information includes all matters of suspected fraud, matters under investigation and completed matters, whether the fraud was proven or not, whether the matter was referred to the CDPP or not, and whether the investigation outcome was a criminal, civil or administrative remedy.

Similarly, with reporting the outcomes of fraud internally, the public reporting of de-identified information helps illustrate contemporary ethical issues, it demonstrates that disciplinary decisions are regarded seriously, while also demonstrating the commitment of the entity to investigate allegations of fraud.

8.2.3. Communication

Once the result of an investigation is known (whether the outcome is a criminal prosecution or an administrative remedy), as far as permitted by privacy legislation, the entity should consider communicating the outcomes to staff (employees and contractors) and, where appropriate, the public (customers, clients and suppliers). This demonstrates that disciplinary decisions are regarded seriously and consistently (key factors in the preparedness of individuals to report wrongdoing in the future) and also serves to keep fraud prevention in the front of the minds of staff and/or customers, clients and suppliers.

Proactive media management may also display the entity’s attitude and response to fraud positively, thus encouraging further external reporting as well as maintaining public confidence that fraud is a serious matter and will be handled accordingly.

Large entities with a significant number of fraud cases should use a communication strategy to plan the reporting of its various types of fraud in order to ensure the information is effective in targeting the relevant audience.

8.3. Monitoring, evaluation and reporting in a program context

The fraud control arrangements established within a program need to be actively monitored and the outcomes of these arrangements reported to the appropriate managers. These monitoring and reporting arrangements should reflect the importance of the program and its identified fraud risks.

Early identification of appropriate data requirements and sources assists in establishing timely and effective monitoring activities. The timely reporting of key issues and trends may have a higher priority than the precise accuracy of underlying data, particularly for high-risk initiatives. The objective of these monitoring activities is to enable an entity to quickly focus attention and resources on emerging issues and will assist in minimising the risks and impacts of fraud.

Evaluation and reporting are essential elements in the closure phase of a program’s life cycle. Reviewing the effectiveness of fraud controls in a program will assist the entity to better administer future programs. Communication of the successes and failures in fraud control initiatives can also benefit other program and service delivery entities.

## BETTER PRACTICE CHECKLIST

### Monitoring, evaluating and reporting

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are there effective reporting channels (internal and external) in place to ensure all reported instances of fraud are adequately monitored?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do the monitoring systems ensure appropriate accountability for fraud control?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a quality assurance review system in place to help identify problems in all aspects of fraud control and its operations?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Following an instance of fraud, does the entity review the work processes subject to the fraud to determine whether changes are required to existing processes, including processes relating to fraud risk assessment and fraud prevention?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key points

- ‘Identity fraud’ has been defined as ‘the gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated identity, a manipulated identity, or a stolen / assumed identity’.

- In response to the threat of identity fraud the Council of Australian Governments agreed to a National Identity Security Strategy, a cross-jurisdictional, whole-of-government approach to combat the misuse of stolen or assumed identities.

- The Australian Crime Commission manages the Australian Identity Protection Register, which captures the details of fraudulent identities from participating law enforcement entities.
9.1. What is identity fraud?

‘Identity fraud’ has been defined as ‘the gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated identity, a manipulated identity, or a stolen / assumed identity’.57

While the term identity fraud has gained prominence throughout the last decade, the fraudulent use of identities has been in existence for some time. For example, submitting a fraudulent claim for social security benefits in the name of a deceased relative or opening a bank account in a false name.

In 2007, an identity fraud report issued by the United Nations58 stated that ‘a substantial amount of identity-related crime is associated with economic fraud, as a means of avoiding fraud prevention measures and avoiding criminal liability and, in most cases, as a means of deception central to the fraud offence itself.’

In response to the threat of identity fraud and identity-related crime and its consequences, the Council of Australian Governments (COAG) agreed in 2005 to develop and implement a National Identity Security Strategy.


The National Identity Security (NIS) Strategy was developed by the COAG in 2005 and is a cross-jurisdictional, whole-of-government approach to combat the misuse of stolen or assumed identities in the provision of government services.59

The six elements of the NIS Strategy, endorsed through an Intergovernmental Agreement (IGA) signed in 2007, address:

- proof of identity and enrolment processes;
- security features on proof-of-identity documents;
- document verification on government databases;
- integrity of information on government databases;
- authentication of individuals accessing services online; and
- biometric interoperability.

The IGA established the National Identity Security Coordination Group (NISCG)—comprising representatives from the Commonwealth, states and territories—to develop the NIS Strategy. Work to develop the NIS Strategy has led to the creation of several best practice / reference guides to improve identity management practices.

These initiatives include the development of the:

- Gold Standard Enrolment Framework as a benchmark for organisations designing and revising enrolment processes. The Framework is applicable to organisations requiring a high level of assurance of a person’s identity before issuing government documents which function as key credentials of proof of identity.

• Security Standards for Proof-of-Identity Documents as a guide for organisations wishing to consider improving the physical security features of key proof-of-identity documents.

• Document Verification Service (DVS) to improve the ability of government organisations across jurisdictions to verify proof-of-information documents. The DVS is a secure, online system which verifies the accuracy and currency of proof-of-identity documents in real time. While the DVS provides a higher level of assurance for organisations enrolling new clients for services, such as Centrelink and the Australian Taxation Office, it is unable to be fully implemented until protocols and agreements are in place with all States and Territories.

• Data Matching Better Practice Guidelines to provide practical advice for data matching practitioners and lead to improved data matching performance and improved data quality.

• Gold Standard e-Authentication Requirements to guide authentication for clients for electronic transactions where the identity risks associated with the transaction require a high level of assurance.

Organisations can obtain further information regarding the strategies by accessing the Commonwealth Attorney-General’s website on Identity Security.

9.3. Commonwealth law enforcement initiatives

Operationally, law enforcement institutions have developed initiatives to assist in combating identity fraud. The Australian Crime Commission (ACC) manages the Australian Identity Protection Register (AIPR) which captures the details of fraudulent identities from participating law enforcement organisations.

The AIPR is used to:

• assist entities in protecting genuine identities;

• assist investigators reduce the incidence of identity fraud;

• identify fraudulent and stolen identities; and

• facilitate cooperation and coordinate the exchange of identity fraud information and intelligence between organisations for the purpose of law enforcement, the protection of public revenue and informing relevant administrative decisions.

A number of law enforcement organisations, including the Australian Crime Commission, Australian Federal Police, Department of Immigration and Citizenship, Australian Customs and Border Protection, and State Police are also working together as part of the Identity Security Strike Teams. The purpose of the strike teams is to target organised identity crime syndicates.

60. In 2009–10, the ANAO completed its performance audit of the coordination of the development of the National Identity Security Strategy by the Attorney-General’s Department.
9.4. Identity fraud risk management options

In recognition of the fact that a purpose of identity fraud is to avoid detection, organisations should ensure that when implementing fraud prevention and detection strategies, consideration is given to the risk of identity fraud. The extent of the fraud prevention and detection strategies will depend on:

- the risk posed by identity fraud on the activities of the organisation; and
- the risk posed to others (whether government, business or individuals) through the organisation issuing a proof-of-identity document to a fraudster which could be used to commit identity fraud.

In addition to the fraud prevention and detection measures discussed in previous chapters, the following are some fraud prevention and detection measures organisations might consider to minimise the risk of identity fraud.

**Know your customer**

A strategy for assisting with the prevention of identity fraud is to identify a customer on initial engagement. The Gold Standard Enrolment Framework developed through the NIS Strategy has been developed to assist organisations with knowing their customers. Organisations should identify what and how much documentation a customer should provide to establish their identity before the provision of services and this information should be publicised.

**Fraud awareness training**

A strategy for assisting with the prevention of identity fraud is training front-line staff to detect fraudulent documentation. Some Commonwealth and State Government documentation contains security features, such as an Australian passport with a computer chip embedded in the document. A working knowledge of, and familiarity with, these security features by front-line staff may assist in the early detection of a fraudulent document.

**Document verification**

A strategy for assisting with the detection of identity fraud is checking the authenticity of a government document. A common technique for fraudsters is the creation of false documentation. The Document Verification Service developed through the NIS Strategy can assist with confirming the authenticity of government documents. The Document Verification Service is expected to expand the number of Commonwealth and state organisations through which checks can be made as more organisations, states and territories sign up to the process.

**Data matching**

A strategy for assisting with the detection of identity fraud is matching entity data with other Commonwealth and state organisations’ data. Data matching allows information from a number of sources to confirm the legitimacy of a person and/or data. Organisations should consider the need to source another’s data, and options for interrogating the data. The Data Matching Better Practice Guidelines developed through the NIS Strategy can assist.

**Integrity of data**

While the strategies above may assist with preventing and detecting identity fraud, this is only as useful as the data which is maintained by an organisation. If an organisation’s data is not accurate and up-to-date, this will create opportunities for fraud to be committed. It is recommended that organisations continually review the currency and accuracy of their data.
**Case Study**

Centrelink and identity fraud

Through careful interrogation of information systems data, Centrelink’s Fraud Intelligence team were able to identify a person using four false identities, in addition to their own, to obtain Centrelink benefits. The person claimed two sets of twins for each false identity (a total of 16 children), one set of false twins in their own name, and their two real children (in total 20 children).

The person worked in a hospital and had access to documentation which could be provided to Centrelink as proof of the birth of a child. In addition, the person produced copies of false death certificates (of alleged spouses) and passports as proof of identity, and fraudulently certified the documents as true using the name of a bogus solicitor.

The person opened bank accounts in the false names using the same fraudulent identification, and used different post office boxes for each claim (a total of five PO boxes).

Centrelink commenced surveillance of the person for the purpose of obtaining evidence linking the person to the false identities. Centrelink referred the person to the Australian Federal Police, who executed search warrants on the person’s homes, post office boxes and banks.

During an interview the person admitted to their actions, was subsequently charged and pleaded guilty in court. The total amount of the fraud exceeded $600,000.
Appendices
Appendix A

Legislation and policies relevant to fraud control

In addition to the Fraud Control Guidelines, the legislative framework for managing fraud incorporates a number of Commonwealth Acts, regulations and policies. The key elements of this framework are listed below.

**Key legislation, regulations and orders**
- Financial Management and Accountability Act 1997
- Financial Management and Accountability Regulations 1997
- Commonwealth Authorities and Companies Act 1997
- Corporations Act 2001
- Public Service Act 1999, including APS Values and Code of Conduct
- Privacy Act 1988

**Other legislated requirements**
- Crimes Act 1914
- Evidence Act 1995
- Director of Public Prosecutions Act 1983
- Auditor-General Act 1997
- Proceeds of Crime Act 2002
- Freedom of Information Act 1982
- Electronic Transaction Act 1999
- Telecommunications (Interception) Act 1979
- Telecommunications (Interception) and Listening Device Amendment Act 1997

**Commonwealth policies**
- Commonwealth Fraud Control Guidelines
- Australian Government Investigation Standards
- Australian Government Protective Security Policy Framework
- Prosecution Policy of the Commonwealth
### Appendix B

**Audit Committee fraud control aide-memoire**

<table>
<thead>
<tr>
<th>Governance arrangements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the entity have an appropriate fraud incident register and associated procedures in place to capture and effectively investigate fraud-related information?</td>
</tr>
<tr>
<td>Does the entity’s fraud control framework integrate with the entity’s risk management and compliance frameworks?</td>
</tr>
<tr>
<td>Is the fraud control framework adequately supported by sufficient instructions and guidance for employees?</td>
</tr>
<tr>
<td>Does the entity have an appropriate fraud awareness and ethics training process in place and is this supported by a robust Fraud Policy and Code of Conduct?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fraud risk assessment and fraud control plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the entity’s fraud risk assessment consider:</td>
</tr>
<tr>
<td>• external and internal fraud risks?</td>
</tr>
<tr>
<td>• the entity’s role and function?</td>
</tr>
<tr>
<td>Is the fraud risk assessment linked to the entity’s risk assessment and business planning process?</td>
</tr>
<tr>
<td>Have key controls been identified and established to address all identified fraud risks?</td>
</tr>
<tr>
<td>Where shortcomings have been identified, have strategies been identified to mitigate these?</td>
</tr>
<tr>
<td>Have the key fraud risks been considered in the context of the entity’s internal audit plan?</td>
</tr>
<tr>
<td>Is the entity’s fraud risk assessment and fraud control plan current and up-to-date?</td>
</tr>
<tr>
<td>Is there a formal process in place to regularly review the entity’s fraud risk assessment and fraud control plan?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitoring and reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there a formal process in place to monitor and report on the fraud risks and controls?</td>
</tr>
<tr>
<td>Does the entity have adequate reporting channels in place for individuals (both internal and external to the entity) to report a suspected fraud?</td>
</tr>
<tr>
<td>Does the Audit Committee receive regular reports on fraud from the entity’s Fraud Manager? (These reports should outline any identified allegations of fraud, the status of any ongoing investigations and any changes to identified fraud risks.)</td>
</tr>
</tbody>
</table>
### Appendix C

**Example of a fraud risk register**

<table>
<thead>
<tr>
<th>Fraud risk description</th>
<th>The fraud risk is described, ensuring that both the cause and impact of the fraud risk eventuating is covered in the description provided.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud risk factors</td>
<td>The fraud risk factors are those conditions or actions which are most likely to cause the fraud risk to eventuate. This will generally be a brief list of likely scenarios that could occur.</td>
</tr>
<tr>
<td>Inherent likelihood</td>
<td>The inherent likelihood provides an indication of how often an identified risk might eventuate in the absence of any controls. This is generally measured using a five-point scale (that is, almost certain, likely, possible, unlikely, rare).</td>
</tr>
<tr>
<td>Inherent consequence</td>
<td>The inherent consequence provides an indication of how serious the consequences would be if an identified risk eventuated in the absence of any controls. This is generally measured using a five-point scale (that is, extreme, major, moderate, minor, insignificant).</td>
</tr>
<tr>
<td>Inherent risk rating</td>
<td>The inherent risk rating provides a ranking for an identified risk once the likelihood and consequence of the risk has been considered in the absence of any controls. This is generally measured using a five-point scale (that is, severe, high, medium, low, very low).</td>
</tr>
<tr>
<td>Key controls identified</td>
<td>The key controls refer to those controls currently established within the entity to minimise the likelihood and consequence of the identified fraud risk eventuating.</td>
</tr>
<tr>
<td>Residual likelihood</td>
<td>The residual likelihood provides an indication of how often an identified risk might eventuate when taking into consideration the effectiveness or otherwise of the existing controls. This is generally measured using a five-point scale (that is, almost certain, likely, possible, unlikely, rare).</td>
</tr>
<tr>
<td>Residual consequence</td>
<td>The residual consequence provides an indication of how serious the consequences would be if an identified risk eventuated when taking into consideration the effectiveness or otherwise of the existing controls. This is generally measured using a five-point scale (that is, extreme, major, moderate, minor, insignificant).</td>
</tr>
<tr>
<td>Residual risk rating</td>
<td>The residual risk rating provides a ranking for an identified risk once the likelihood and consequence of the risk has been considered after taking into consideration the effectiveness or otherwise of the existing controls. This is generally measured using a five-point scale (that is, severe, high, medium, low, very low).</td>
</tr>
<tr>
<td>Fraud risk owner</td>
<td>The fraud risk owner is the individual / group within the entity with accountability for managing the identified fraud risk.</td>
</tr>
<tr>
<td>Action required</td>
<td>This relates to the identification of any further actions that the entity must undertake in relation to the identified fraud risk (that is, new controls to be established).</td>
</tr>
</tbody>
</table>
Appendix D

Recent ANAO audits related to fraud control


Appendix E

Bibliography


Attorney-General’s Department, *Commonwealth Fraud Control Guidelines*, Canberra, 2011.


Australian National Audit Office, Better Practice Guide—Public Sector Audit Committees – Having the right people is the key, ANAO, Canberra, 2005.


The Audit Office of New South Wales, *Fraud Control Improvement Kit—Meeting Your Fraud Control Obligations*, Sydney, 2006.


Index
A

ABC fraud surveys, 40
counting reports, 53, 57
active fraud detection, 56–60
administrative remedies, 70
AFP see Australian Federal Police
AGIS, 64, 66–8
Airservices Australia ethics hotline, 55
allegations see fraud allegations
ANAO see Australian National Audit Office
Annual Report to Government (AIC fraud survey), 19, 53, 78
annual reports, 77–8
anti-corruption programs, 47
APS Code of Conduct, 10–11, 15–16, 41
fraud awareness training, 43–4
non-government service providers, 45–6
whistleblowing and, 56
APS Values, 10–11, 15–16, 41
fraud awareness training, 44
non-government service providers, 45–6
AS 4811-2006 Employment Screening and the
Australian Government Protective Security Policy
Framework, 42
AS 8001-2008 Fraud and Corruption Control, 36,
46–7, 49, 56, 65
AS/NZS ISO 31000:2009 Risk Management
Principles and Guidelines, 36, 48
assessments see fraud risk management;
preliminary case assessments
Attorney-Generals Department, 19
Audit Committees, 21, 22, 90
audits, 58, 92
Australian Broadcasting Corporation
fraud surveys, 40
Australian Customs and Border Security
case study, 45
Australian Federal Police, 19
Case Categorisation and Prioritisation Model, 63
identity fraud initiatives, 84
referrals to and assistance from, 63–4, 67
Australian Government Investigations Standards
(AGIS), 64, 66–8
Australian Identity Protection Register (AIPR), 84
Australian Institute of Criminology, 19, 53, 78
Australian National Audit Office (ANAO), 19, 59
see also Better Practice Guide
fraud surveys, 34
recent audits, 92
Australian Standards see AS...; AS/NZS...;
Australian Government Investigations Standards
authentication requirements, 83–4

B

benefits of loss recovery, 71
Better Practice Guide, 2–5, 41, 59
checklists, 24, 50, 60, 72, 79
Bibliography, 93–4
Boards of Directors, 20

C

CAC Act see Commonwealth Authorities and
Companies Act 1997
‘CA/CM’ (continuous auditing / continuous
monitoring), 58
case assessments, preliminary, 66
Case Categorisation and Prioritisation Model
(CCPM), 66
case studies, 5
ABC fraud surveys, 40
Airservices Australia ethics hotline, 55
Centrelink and identity fraud, 86
Customs Z Card case study, 45
DCCEE fraud response, 72
DVA Integrity Sub-committee, 22
FahCSIA fraud response governance model, 65
central agencies, role of, 19
Centrelink and identity fraud, 86
checklists see Better Practice Guide, checklists
Chief Executive Officers (CEOs)
accountability for fraud control, 20
FMA Act and, 15
INDEX

A
amounts, 3
 Atomic Energy Act, 72
Audit Office, 17
AUPs see APS Code of Conduct
B
better practice, 10
binoculars, 64
CA/CM see continuous auditing / continuous monitoring
C
civil remedies, 70
codes of conduct
   APS see APS Code of Conduct
   non-government service providers, 45–6
Commonwealth authorities, 17
Commonwealth Authorities and Companies Act 1997 (CAC Act), 15, 17
   accountability for fraud control, 20
   ANAO audits, 19
   applicability of Fraud Control Guidelines, 18
Commonwealth companies, 17
Commonwealth Director of Public Prosecutions, 19, 69–70
Commonwealth Fraud Control Guidelines, 2–3, 15
   applicability of, 18
   monitoring and reviewing fraud risk, 37
   objectives of, 18
   policy framework, 18
Commonwealth Fraud Control Policy, 2
communication
   about outcomes of investigations, 78
   of identified fraud, 47–8
   to program staff, 49
   risk management process, 36–7
complex fraud
   detection, 53
   investigation, 63–4
costs
   Losses, 32
   of identified fraud, 47–8
   of program fraud, 73
   of program risks, 37
   of reported fraud, 47–8
costly theft, 71
credibility
   of identified fraud, 47–8
   of intelligence, 63
D
data integrity, 85
data matching, 58–9, 85
data mining, 57–9
Department of Climate Change and Energy
   Efficiency Fraud Response, 72
Department of Veterans’ Affairs (DVA) Integrity Subcommittee, 22
detection
   see fraud monitoring, reporting and evaluation
deterrent effect
   of fraud responses, 47–8, 69–71
   of fraud responses, 72
Directors, 20
document verification, 83–5
documenting risks, 37
duty of care, 17
E
e-commerce, 1, 28
effectiveness of fraud control plans, 76
employees, 3
   allegations by, 54
   early warning of fraud, 56–7
   screening of, 42
enrolment processes, 83–4
entities, 67
   change in structure or function, 34
   ‘fit for purpose’ approach, 39, 43
   fraud risks, 33–5
   partnering to share information, 59
ethical culture see organisational ethical culture
evaluation
   see fraud monitoring, reporting and evaluation
external fraud, 34–5
identity fraud, 85
screening, 46–7
Customer Z Card case study, 45
evidentiary requirements for prosecution, 70
Executive, 2, 9, 20
see also Chief Executive Officers
external fraud, 19, 34, 53, 58–9
external parties, 54, 58–9
external reporting, 77–8
external service providers, 59

F
FaHCSIA fraud response governance model, 65
Financial Management and Accountability Act 1997 (FMA Act), 15–16
accountability for fraud control, 20
external reporting, 77–8
strategies, 19
financial statement audits by ANAO, 19
fraud
communication of identified fraud, 47–8
defined, 1, 18
financial losses, 77
loss recovery, 70–1
perpetrators of, 2
prosecution for, 17–18, 69–70
response to, 27–8, 61–72, 76
fraud allegations
by employees, 54
by external parties, 54
fraud incident registers, 65
hot spot analysis, 57
mechanisms for reporting, 54
preliminary case assessment, 66
fraud awareness training, 42–4
Customs Z Card case study, 45
identity fraud and, 85
program staff, 49
fraud control, 1–2, 25–8, 37–8
see also governance structures
Audit Committee aide-memoire, 22, 90
framework, 3–4
high-risk areas and programs, 46–7, 49
legislation and policies relevant to, 89
outsourcing, 39
program-specific fraud controls, 28
recent ANAO audits, 92
reporting outcomes of, 77–8
Fraud Control Guidelines see Commonwealth Fraud Control Guidelines
fraud managers, 2, 20–1
fraud monitoring, reporting and evaluation,
27, 54, 73–9
checklists, 79
communication of identified fraud, 47–8, 78
continuous auditing / continuous monitoring, 58
external fraud, 58–9
fraud detection, 27–8, 51–60, 85
fraud hotlines, 54–5
fraud identification, 65, 68
fraud incident registers, 65
fraud indicators, 56–8
internal fraud, 56–7
investigations, 63–9
monitoring fraud risk assessment, 37
fraud prevention, 27–50
Better Practice Checklist, 50
built into program design, 48–9
‘fit for purpose’ approach, 31
identity fraud, 85
policies, 2, 13, 16, 18, 40, 89
strategic fraud control, 27–8
fraud risk management, 32–40
ABC fraud surveys, 40
assessments, 36–7, 75
built into program design, 48–9
early warning signs, 56–7
exposure to risk, 34–5
fraud risk register, 91
high-risk areas, 46–7, 49
hot spot analysis, 57, 65
identity fraud, 81–6
prevention measures targeted to risk, 31–2
fraud surveys
Australian Institute of Criminology, 19, 53, 78
Australian National Audit Office, 34
KPMG Fraud and Misconduct Survey 2010:, 53–4

G
good faith, 17
governance structures, 13, 20–4
Audit Committee aide-memoire, 22, 90
Better Practice Checklist, 24
linking fraud control across, 23

H
high-risk areas, 46–7, 49
historical data analysis, 58
Home Insulation Program case study, 72
hot spot analysis, 57, 65
hotline facilities, 54–5

I
identified fraud, communication of, 47–8, 78
identity fraud, 5, 81–6
Centrelink and, 86
defined, 83
risk management options, 85
indicators of fraud see fraud risk management

J
justification for fraud, 20

L
law enforcement initiatives in identity fraud, 84
leadership, 3–4, 7, 9–10, 20–1
legislative framework, 2, 13, 15–18, 89
line area employees, 3
linking fraud control across governance structures, 23
losses due to fraud, 70–1, 77

M
management see Executive; leadership
management accounting reports, 57
media reporting, 48, 78
members of the public, allegations by, 54
minor fraud, 63
misconduct, remedies for, 70
monitoring see fraud monitoring, reporting and evaluation
motivation for fraud, 20

N
National Identity Security Strategy (COAG), 83–4
non-government service providers, 45–6, 59

O
operational managers, 3
opportunity for fraud, 20
organisation size, 39
organisational ethical culture, 3–4, 7, 10–11, 43
organisational risks, 32–3
organisational structure see governance structures
organisation-wide planning, 32–3
outsourcing, 39, 59, 67
ownership of risks, 37
partnering with other entities, 59
passive fraud detection, 53–6
performance audits by ANAO, 19
perpetrators of fraud, 2
police see Australian Federal Police
policies on fraud see fraud risk management
post transactional reviews, 57–8
preliminary case assessments, 66
prevention see fraud prevention
private sector providers, 45–6, 59
Proceeds of Crime Act 2002, 71
procurement, 28, 35, 41
program design and management, 1, 5, 25–8
change in structure or function, 34
fraud control strategies, 27–8, 48–9, 60
fraud response in, 71
monitoring, evaluation and reporting and, 78
non-government service providers, 45–6
program-specific fraud controls, 28, 32
proof of identity processes, 83–4
prosecution for fraud, 17–18, 69–70
public interest disclosures, 56
public interest to prosecute, 70
Public Service Act 1999, 15–16, 56, 70

rationalisation for fraud, 20
recording fraud (registers), 65
recovery action, 70–1
‘red flags’ (early warnings), 56–7
referrals to AFP, 63–4, 67
registers of fraud risk, 91
regulations see legislative framework
remedies, civil and administrative, 70
reporting see fraud monitoring, reporting and
evaluation
reports see management accounting reports
resources for fraud detection and control, 31–2, 53
response see fraud prevention; fraud risk
management
retrospective review, 58
reviewing activities, 37, 56–9
risk management see fraud risk management
risk registers, 91
risks see fraud risk management
routine fraud, 63

screening employees, 42
Secretaries, accountability of, 20
security controls, 32–3
senior executives see Executive
serious fraud, 63–4
service provision see non-government service
providers; program design and management
small entities, 39
staff members see employees
Standards see AS...; AS/NZS...; Australian
Government Investigations Standards
strategic fraud control, 27–8
suppliers see non-government service providers;
procurement

technology in service delivery, 1, 28
tip-off facilities, 54–5
‘traditional’ fraud control, 10
training, 69
see also fraud awareness training

Values see APS Values

warning signs, 56–7
whistleblowing, 56
whole of agency risk management, 32–3
Fraud Control in Australian Government Entities

The Financial Management and Accountability Act 1997 and the Commonwealth Authorities and Companies Act 1997 were replaced by the Public Governance, Performance and Accountability Act 2013 (PGPA Act) and supporting rules on 1 July 2014. The PGPA Act provides a common legislative framework for the governance, performance and accountability of all Commonwealth entities.

The ANAO will commence updating this Guide in 2014-15, in consultation with the Attorney-General’s Department, to reflect the PGPA Act and other policy and administrative changes in relation to the management of fraud.

Further information on the PGPA Act is available at:
www.pmra.finance.gov.au