Australian Government
Attorney-General's Department

Preventing, detecting and dealing with fraud

Resource Management Guide No. 201

AUGUST 2017

Resource Management Guide No. 201 - Preventing, detecting and dealing with fraud

This guide supports the Fraud Rule and Fraud Policy and is considered best practice for all Commonwealth entities. This guide was reissued in August 2017.

Contents

Audience

This guide is relevant to

- accountable authorities and Commonwealth officials involved in fraud control arrangements within Commonwealth entities
- fraud control practitioners interested in better practice guidance.

Key points

This guide:

- is issued by the Attorney-General's Department to assist accountable authorities to meet their obligations under the *Public Governance, Performance and Accountability Act 2013*, Fraud Rule and the Fraud Policy
- together with the Fraud Rule and Fraud Policy, forms part of the Commonwealth Fraud Control Framework
- provides better practice guidance for accountable authorities and Commonwealth officials on fraud control arrangements within entities
- is available on AGD's website at *www.ag.gov.au/fraud*.

Abbreviations and acronyms

ACCC	Australian Competition and Consumer Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGIS	Australian Government Investigations Standards
AIC	Australian Institute of Criminology
ANAO	Australian National Audit Office
ASIC	Australian Securities and Investments Commission
CCPM	Case Categorisation and Prioritisation Model
CCE	corporate Commonwealth entity
CDPP	Commonwealth Director of Public Prosecutions
NCE	non-corporate Commonwealth entity
PGPA Act	*Public Governance, Performance and Accountability Act 2013*
PGPA Rule	*Public Governance, Performance and Accountability Rule 2014*

Glossary

accountable authority: the person or group of persons who has responsibility for, and control over, an entity's operations as set out under section 12 of the PGPA Act.

Commonwealth official: an individual who is in, or forms part of, the entity as set out under section 13 of the PGPA Act.

entity: a department of state, a parliamentary department, a listed entity or a body corporate established by a law of the Commonwealth.

corporate Commonwealth entity: a Commonwealth entity that is a body corporate and legally separate from the Commonwealth.

the Framework: the Commonwealth Fraud Control Framework

Fraud Policy: Commonwealth Fraud Control Policy.

Fraud Rule: Section 10 of the PGPA Rule.

non-corporate Commonwealth entity: a Commonwealth entity that is not a body corporate but is legally part of the Commonwealth.

Resources

Other relevant publications include:

- Australian Government Investigations Standards
- Australian Public Service Code of Conduct
- Case Categorisation and Prioritisation Model
- Commonwealth Fraud Control Policy
- Commonwealth Risk Management Policy
- Prosecution Policy of the Commonwealth
- Protective Security Policy Framework
- Resource Management Guide No.214 – Notification of significant non-compliance with the finance law (PGPA Act, section 19)

The words '**must**', '**required**', '**requires**' and '**requiring**' denote mandatory compliance by accountable authorities/officials. The use of the words 'could', 'may', 'encouraged' or 'consider' convey non-mandatory guidance. The guidance to which these words relate may or may not be applied by accountable authorities/officials in their approach to resource management, depending on the operating circumstances of the entity and its appetite for risk.

Introduction

1. Fraud against the Commonwealth is a serious matter for Commonwealth entities and the community. Not only can it constitute a criminal offence, but fraud reduces funds available for delivering public goods and services, undermines the integrity of government and can place public safety at risk. The Australian community rightly expects that entities and officials acknowledge and fulfil their responsibilities as stewards of public funds and make every effort to protect public resources.

2. This guide is issued by the AGD as better practice to assist accountable authorities to meet their obligations under the Fraud Rule and Fraud Policy. This guide expands on the Fraud Rule and Fraud Policy to articulate a flexible framework for fraud control that can be tailored to the circumstances and needs of different entities while providing coherent, consistent and transparent requirements and maintaining accountability.

3. Where the guide uses the term 'must', this reflects a pre-existing obligation. If a conflict arises between this guide and legislation or Commonwealth policies, the legislation or policy takes precedence.

Part 1 – The legislative framework

4. The Fraud Rule provides a legislative basis for the Commonwealth's fraud control arrangements. It sets out fraud control requirements to assist accountable authorities to meet their obligations under the PGPA Act. Breaches of the Fraud Rule may attract criminal, civil, administrative and disciplinary remedies (including under the PGPA Act, the *Public Service Act 1999*, the *Criminal Code Act 1995* and the *Crimes Act 1914*).

5. Under section 21 of the PGPA Act, NCEs are also required to be governed in a way that is not inconsistent with polices of the Australian Government, which includes the Fraud Policy.

6. Guidance material in this guide is non-binding. It sets out better practice around fraud control to assist accountable authorities to meet their obligations under the PGPA Act. This guide can be read in conjunction with other relevant Commonwealth polices and guides.

7. Failure to maintain appropriate fraud control arrangements within an entity may constitute significant non-compliance with the finance law.[1]

---

[1] For the purpose of the PGPA Act, the finance law comprises of:
- the PGPA Act
- the PGPA Rule
- an Appropriate Act, and
- any other instrument made under the PGPA Act (for example: Commonwealth Procurement Rules, Commonwealth Grants Rules and Guidelines and PGPA (Financial Reporting) Rule 2015 ; accountable authority instructions under section 20A; determinations establishing special accounts under section 78; determinations transferring functions between non-corporate Commonwealth entities under section 75; and government policy orders under sections 22 or 93)

Roles and responsibilities of key entities

- AFP investigates most serious or complex crime against Commonwealth laws, including internal and external fraud against the Commonwealth. The AFP can also conduct quality assurance reviews of entities' fraud investigations and provide advice and assistance to entities investigating fraud, including recovery action under the Proceeds of Crime Act 2002.
- CDPP is responsible for prosecuting offences against Commonwealth law.
- AGD provides advice to the Government about fraud control arrangements within the Commonwealth. Its role includes developing and reviewing general policies of the Government with respect to fraud control and advising entities on those policies.
- ANAO has the authority to conduct performance audits of Commonwealth entities that may include an assessment of how entities meet their fraud responsibilities.
- AIC is responsible for conducting an annual fraud survey of entities and producing reports on fraud against the Commonwealth, Commonwealth entity compliance with the Framework and fraud trends.
- ACLEI supports the Integrity Commissioner to detect and prevent corrupt conduct, and to investigate corruption issues, in prescribed Commonwealth entities with law enforcement functions. Internal and complex fraud incidents in these entities may also be regarded as corrupt conduct and be referred to ACLEI.
- ACCC is responsible for enforcing compliance with Australia's competition laws, which contain criminal and civil prohibitions on fraud in the form of cartel conduct. Cartel conduct occurs when competitors conspire to fix or control prices, rig bids, restrict supply or allocate markets. The ACCC is committed to providing procurement officers within entities with the knowledge and the tools needed to detect and report possible collusion by suppliers.
- ASIC regulates Australian companies, financial markets, and financial services organisations and professionals who deal with and advise on investments, superannuation, insurance, deposit taking and credit under a number of Commonwealth laws. ASIC uses enforcement powers to detect and deal with unlawful conduct and responds to breaches of law ranging from minor regulatory offences through to serious misconduct. Entities can contact ASIC where fraud matters involve any of the above conduct.

Part 2 – Objectives and scope

8. The Commonwealth is committed to a targeted and risk based approach to prevent and detect fraud perpetrated against the Commonwealth. Managing fraud risk is a collective responsibility of all Commonwealth officials.

9. The objectives of the Fraud Rule, Fraud Policy and this guide are to:

- protect public resources, including information and property, and
- protect the integrity and good reputation of entities and the Commonwealth.

This includes reducing the risk of fraud occurring, discovering and investigating fraud when it occurs, and taking appropriate corrective actions to remedy the harm.

10. The Fraud Rule, Fraud Policy and this guide establish the fraud control framework within which entities determine their own specific arrangements to control fraud against them.

11. Fraud control in the Commonwealth is based on:
    - thorough regular assessment of risks particular to the operating environments of entities and the programs they administer
    - developing and implementing processes and systems to effectively prevent, detect and investigate fraud
    - applying appropriate criminal, civil, administrative or disciplinary action to remedy the harm from fraud and deter future fraud
    - recovering proceeds of fraudulent activity, and
    - providing fraud awareness training for all officials and specialised training of officials involved in fraud control activities.

12. This guide sets out better practice that entities are expected to utilise in their fraud control arrangements taking into account their individual circumstances, and applying a common sense approach. Entities are strongly encouraged to ensure all their officials engaged in fraud control are aware of and have access to this guide.

13. The guide is not intended to cover all types of entity risk. For instance, where corruption or other entity risks are concerned, this guide acts as a starting point to be used in conjunction with other appropriate guidance materials. However, fraud risks and controls are often linked in with other related risks, including protective security and corruption. Fraud controls may be integrated within an overall general business risk approach as described in the Commonwealth Risk Management Policy.

Part 3 – Definition of fraud

14. Fraud against the Commonwealth is defined as 'dishonestly obtaining a benefit, or causing a loss, by deception or other means'.[2] This definition is based on the dishonesty offences under chapter 7 of the Criminal Code.

15. Fraud against the Commonwealth may include (but is not limited to):
    - theft
    - accounting fraud (e.g. false invoices, misappropriation)
    - misuse of Commonwealth credit cards
    - unlawful use of, or unlawful obtaining of, property, equipment, material or services
    - causing a loss, or avoiding and/or creating a liability

[2] Paragraph viii. Commonwealth Fraud Control Policy

- providing false or misleading information to the Commonwealth, or failing to provide information when there is an obligation to do so
- misuse of Commonwealth assets, equipment or facilities
- cartel conduct
- making, or using, false, forged or falsified documents, and/or
- wrongfully using Commonwealth information or intellectual property.

16. Fraud requires intent. It requires more than carelessness, accident or error. When intent cannot be shown, an incident may be non-compliance rather than fraud.

17. A benefit is not restricted to a material benefit, and may be tangible or intangible, including information. A benefit may also be obtained by a third party.

18. **Internal fraud** is where fraud against an entity is committed by its officials or contractors. Fraud by an official is likely to represent significant non-compliance with the finance law as the official would have breached the general duty of an official under section 26 of the PGPA Act to act honestly, in good faith and for a proper purpose in perpetrating the fraud.

19. **External fraud** is where fraud comes from outside the entity from external parties such as clients, service providers, other members of the public or organised criminal groups.

20. Entities are advised to be alert to the risk of **complex fraud** involving collusion between their officials and external parties. Complex fraud can include instances when an official or group of officials:
    - are targeted and succumb to exploitation by external parties (bribery, extortion, grooming for favours or promises), or
    - initiate the misconduct (including through external parties infiltrating the entity).

21. Fraud can include corrupt conduct where the conduct results in a party obtaining a benefit from, or causing a loss to, the Commonwealth. An example of this is collusion between a Commonwealth official and a contractor. However, some forms of corrupt conduct, such as soliciting for bribes or secret commissions, may not cause a direct financial loss to the Commonwealth, but may distort the market for fair provision of services or inflate prices, and may damage Australia's international reputation and the public's trust in the Government. However, not all corrupt conduct falls under the definition of fraud.

22. By contrast, **trivial fraud** (less significant) refers to matters that may technically meet the definition of fraud but are not serious enough to warrant any formal action beyond a managerial response. Entities are encouraged to take a common sense approach to handling trivial fraud matters. Trivial matters would generally not warrant inclusion in reporting to Ministers under section 19 of the PGPA Act or the AIC as part of its fraud survey. However, it is important for entities to be mindful that incidents of 'trivial fraud' could be the visible indicators of more systemic problems or vulnerabilities.

23. Fraud can simultaneously be a criminal offence, a breach of the Australian Public Service Code of Conduct or duties of officials under the PGPA Act, and/or a breach of contract or other wrong amounting to a civil action.

Dishonesty in the Criminal Code

Part 7.3 in chapter 7 of the Criminal Code deals with fraudulent conduct against the Commonwealth, and contains a range of offences, including:

- dishonestly obtaining a financial advantage from a Commonwealth entity by deception (section 134.2)
- doing anything with the intention of dishonestly:
  - obtaining a gain from a Commonwealth entity, or
  - causing a loss to a Commonwealth entity (sections 135.1(1) and (3))
- conspiring with another person with the intention of dishonestly:
  - obtaining a gain from a Commonwealth entity, or
  - causing a loss to a Commonwealth entity (sections 135.4(1) and (3))
- dishonestly influencing a Commonwealth public official in the exercise of their duties (section 135.1(7)), or
- obtaining a financial advantage which the recipient knows or believes they are not eligible to receive (section 135.2(1)).

The meaning of dishonesty is set out in section 130.3 as follows:

(a) dishonest according to the standards of ordinary people, and

(b) known by the defendant to be dishonest according to the standards of ordinary people.

Part 4 – Role of accountable authorities

24. The primary responsibility for ensuring entities have appropriate fraud control arrangements rests with accountable authorities. Accountable authorities play a key role in setting the ethical tone within their entities, and fostering and maintaining a culture of fraud awareness and prevention. However, effective fraud control requires the commitment of all officials, contractors and third-party providers.

25. Under the PGPA Act, the accountable authority must govern the entity in a way that promotes: the proper use and management of public resources; the achievement of the purposes of the entity; and the financial sustainability of the entity. They must establish and maintain an appropriate system of risk oversight and management, and an appropriate system of internal controls for the entity, including implementing measures directed at ensuring officials of the entity comply with the finance law. They must also be satisfied that their entities comply with the mandatory requirements in the Fraud Rule.[3]

26. All officials, including accountable authorities, must act in good faith and for proper purpose, and not improperly use their position or information.[4]

[3] Sections 15-16 PGPA Act.
[4] Sections 25-29 PGPA Act

Part 5 – Risk assessment

27. Under paragraph (a) of the Fraud Rule, a fraud risk assessment must be conducted regularly and when there is a substantial change in the structure, functions or activities of the entity. Substantial changes can include machinery of government changes and changes to service delivery models, such as expansion of, or into, online provision of information and services.

28. Entities are responsible for determining the risk assessment approach that is most appropriate for their circumstances. Risk assessment processes ideally take into account all significant factors likely to affect an entity's exposure to risk including what assets (including information) need protection and what internal and external pressures affect risk. Subject to an entity's individual risks, entities are encouraged to conduct risk assessments at least every two years. Entities responsible for activities with a high fraud risk may wish to assess risk more frequently.

Common areas where fraud risks can arise include:

- policy and/or program development
- procurement, including tendering and managing supplier interfaces
- revenue collection and administrating payments to the public
- service delivery to the public, including program and contract management
- provision of grants and funding agreements
- exercising regulatory authority
- provision of identification documents
- internal governance arrangements, and
- changes in the activities or functions of an entity.

29. It is important for risk assessment strategies to be reviewed and refined on an ongoing basis in light of experience with continuing or emerging fraud vulnerabilities. The outcomes of fraud risk assessments can be provided to entities' internal audit units and audit committees for consideration in the annual audit work program.

30. Entities generally face different fraud control issues depending on their size and the nature of their business, both of which influence an entity's potential exposure to fraud. It is not always practical to institute measures to address every possible business risk, including potential fraud. Therefore, it is important to carefully assess the likely occurrence of fraud and its impact on an entity's key organisational objectives and core business. A risk based approach enables an entity to target its resources, both in prevention and detection, at problem areas.

31. It is important to avoid looking at fraud in isolation from the general business of the entity. Entities are strongly encouraged to develop dynamic fraud risk assessment procedures integrated within an overall general business risk approach rather than in a separate program. However, some entities or programs will have an inherent risk of fraud due to the nature of their business. Those entities are encouraged to consider developing a fraud risk assessment process that is specific to a particular policy or program area, particularly when developing a new program or policy.

32. Risk assessment is a continuous process. Where appropriate, entities can use a rolling program of updating their risk assessment procedures and risk mitigation measures. In developing their fraud risk assessment and fraud control plan, entities are encouraged to consider the relevant recognised standards: currently 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.

33. Under paragraph (c) (ii) of the Fraud Rule, the risk of fraud is to be considered when planning and conducting the activities of entities. This includes when major new policies are being developed or when there is a significant change in a policy or in the way a policy will be implemented. The assessment of fraud risks is an integral part of program design. It is important for program design to include measures to prevent fraud from occurring. Fraud can also be considered in the context of other business risks.

34. Risk assessment and fraud control planning require specific expertise. Risk assessments can be undertaken using in-house resources, but it is important to ensure that the risk assessment team has access to the range of skills, knowledge and experience necessary to provide coverage of the categories of risk to be considered.

35. If resources are not available in-house, entities may choose to outsource all or part of the risk assessment and fraud control planning process. However, consistent with PGPA Act responsibilities, outsourcing does not remove the responsibility of the accountable authority or of senior management to manage fraud risk. For this reason, entities are encouraged to have a senior official oversee the process, and to ensure that relevant corporate knowledge is appropriately captured and taken into account during the risk assessment and fraud control planning process.

Part 6 – Fraud control plans

36. Under paragraph (b) of the Fraud Rule, fraud risk assessments must be followed by the development (or update) and implementation of a fraud control plan to deal with identified risks. It is important for fraud control plans to emphasise prevention. Fraud control plans are encouraged to be available and accessible to all officials.

37. Fraud control plans and processes do not have to be developed as standalone documents. The fraud control plan can be integrated into the entity's strategic plan, business plan or risk management plan. Specific fraud control plans are encouraged to be made for areas with a high risk within an entity.

38. The fraud control plan can document the entity's approach to controlling fraud at a strategic, operational and tactical level, and encompass awareness raising and training, prevention, detection, reporting and investigation measures.

Fraud control plans may cover:

- a summary of fraud risks and vulnerabilities associated with the entity
- treatment strategies and controls put in place to manage fraud risks and vulnerabilities
- information about implementing fraud control arrangements within the entity
- strategies to ensure the entity meets its training and awareness needs
- mechanisms for collecting, analysing and reporting fraud incidents
- protocols for handling fraud incidents, and
- an outline of key roles and responsibilities for fraud control within the entity.

39. Controls and strategies outlined in fraud control plans are ideally commensurate with assessed fraud risks. Testing controls may indicate that not all controls and strategies are necessary or that different approaches may have more effective outcomes. Controls can often be reviewed on a regular basis to make sure they remain useful.

40. Fraud control arrangements can reflect the fraud risk profile of an entity or particular program. While the nature and extent of fraud risks faced by smaller entities may differ from the fraud risks facing larger entities, these risks will still require targeted mitigation strategies. Entities are encouraged to adopt fit-for-purpose mechanisms to address specific fraud risks.

41. Additionally, fraud control plans can include review and oversight mechanisms to enable entities to evaluate the effectiveness of fraud control strategies regularly, particularly following changes in business processes or systems or after instances of fraud have been discovered. This will help ensure that control systems remain appropriate, cost-effective and proportionate to the actual risks they are addressing.

42. It is important for entities to consider strategies to mitigate the risk of identity fraud as part of their fraud control plans where relevant. The creation and use of fraudulent identity documents can have downstream consequences to other entities and the broader community, such as money laundering or other serious crimes. Entities are encouraged to consider the National Identity Proofing Guidelines as a better practice framework for identity verification processes and use online services such as the Document Verification Service to improve detection of fraudulent identities. Further guidance on managing identity related risks can be found in the National Identity Security Strategy, which seeks to establish nationally consistent processes for enrolling, securing, verifying and authenticating identities and identity credentials.

Part 7 – Fraud prevention, awareness and training

Prevention

43. Fraud prevention involves putting into place effective accounting and operational controls, and fostering an ethical culture that encourages all officials to play their part in protecting public resources. Establishing an ethical culture is an important factor in preventing and detecting fraud. Accountable authorities are strongly encouraged to

foster this culture in their senior leadership specifically, as well as across staff more generally.

Fraud strategy statements can include:

- the definition of fraud
- a statement of the entity's commitment to preventing and controlling fraud
- a statement of officials' and contractors' responsibilities
- a summary of the consequences of fraud
- an assurance that allegations and investigations will be handled confidentially
- directions on how allegations and incidents of fraud are to be reported and managed, and
- advice on where further information can be found.

44. The Fraud Rule requires the accountable authority to ensure that officials in the entity are made aware of what constitutes fraud. A widely distributed fraud strategy statement can assist in raising awareness.

45. Taking fraud into account in the development of policy and programs helps prevent fraud occurring. It is important that entities understand the risks that may impact policy development and are aware of key areas that may lead to vulnerabilities in programs and policies. Examples of these areas are set out in the text box below. Preventative measures can include identity verification measures and early intervention in a matter before non-compliance escalates to fraud. Prevention methods can be built into internal and external policy design. It is also important entities ensure their policies and programs are developed to encourage compliance and avoid perverse incentives creating opportunities for fraud. Entities are encouraged to include fraud prevention in any policy and program development training for officials.

Red flags for policy design

The following list provides examples of factors that may lead to fraud vulnerabilities in programs or policies:

- Systems managed across different government portfolios, service providers and/or jurisdictions
- Opportunities for exploitation by professional facilitators e.g. brokers and agents
- Programs creating new opportunities for unregulated industries
- Programs significantly expanding a regulated industry to new organisations
- Programs requiring verification/authentication of identity, particularly online
- Programs involving electronic claims, submissions, assessments, verification and/or payments
- Programs providing assistance to vulnerable people
- Programs with low verification thresholds, and
- Programs needing to be delivered quickly

Awareness-raising

46. Entities are encouraged to have all officials take into account the need to prevent and detect fraud as part of their normal responsibilities. Appropriate mechanisms could include fraud awareness and integrity training in all induction programs and a rolling program of regular fraud awareness and prevention training for all officials. This training can include information on red flags for internal and external fraud, in addition to how to respond to the red flags. It is also important for entities to have officials involved in policy and program development capable of understanding and managing risk. Training these officials in managing risk can help entities develop better policies and programs by mitigating fraud risks and impacts. Training can also cover ethics, privacy and relevant codes applicable to the entity, such as the APS Code of Conduct, and the roles and responsibilities of other entities, including the AFP and the CDPP.

47. It is useful for entities to evaluate awareness and training initiatives to determine whether they have been successful and the participants have an improved awareness of fraud control and their responsibilities.

48. The Fraud Policy requires NCEs to clearly document their procedures and instructions that assist officials to deal with fraud. Such documents are an important part of effective fraud control and it is important to keep them up-to-date and available to all officials. For this reason, CCEs are strongly encouraged to follow this requirement.

49. Having effective outreach programs can help entities prevent fraud. Outreach activities include entities clearly explaining their integrity policies and programs, and position on fraud to clients and service providers, and where appropriate, to members of the public.

50. It is beneficial for awareness-raising programs for third-party providers to take into account the work they do directly for entities and the services they deliver on behalf of

the entity. These programs can be extended to provide clients and providers information about their rights and obligations, including information on their fraud control responsibilities.

Training for fraud control officials

51. It is important for officials who are primarily engaged in preventing, detecting and/or investigating fraud to be appropriately skilled and experienced.

Investigators

52. The Fraud Policy requires NCEs to ensure that officials engaged in investigating fraud against the Commonwealth meet the required fraud control competency requirements set out in the Australian Government Investigations Standards. This is to ensure the integrity of investigations. For this reason, CCEs are strongly encouraged to follow these requirements.

53. If officials entering these roles do not have relevant experience, it is important for them to receive relevant training as soon as possible, preferably within 12 months of being engaged in these roles. Until an official has attained the relevant qualifications, entities are encouraged to ensure that appropriate supervision is provided.

54. It is important for entities to ensure they have the appropriate authorisations in place to investigate a matter (whether internal or external) with the appropriate level of managerial oversight. Unqualified investigators may compromise a case by:
    - failing to collect all the available evidence
    - collecting evidence in a manner that is inadmissible in court, and/or
    - prematurely alerting the suspect before all available or necessary evidence can be collected.

Fraud control officials

55. The Fraud Policy requires NCEs to ensure officials engaged primarily in fraud control activities possess or attain relevant qualifications or training to effectively carry out their duties. This is to ensure officials are appropriately skilled. For this reason, CCEs are strongly encouraged to follow this requirement.

56. Relevant training and qualifications vary for entities depending on their risks. It is important that officials engaged in these areas are able to identify their entity's fraud risks and develop appropriate and meaningful fraud controls for those risks. It is important that relevant officials do not oversimplify this by following a compliance checklist without applying a common sense approach or considering broader fraud risks to the entity or Commonwealth. Relevant training can include a Certificate IV in Government (Fraud Control) or equivalent qualification for officials implementing fraud control, or a Diploma of Government (Fraud Control) or equivalent qualification for officials managing fraud control.

57. It is important for entities to ensure officials engaged in fraud control have ongoing professional development to further develop their expertise and ensure their skills remain current. Timeframes for refreshing employee knowledge and skills can be determined by entities, ideally occurring at least every three years. Entities with a

greater exposure to fraud may consider developing specialised training programs for these officials to ensure the potential risks to their business are minimised.

58. Officials who perform some fraud control functions, but are not primarily engaged in fraud control or investigation, do not need to attain full qualifications. Entities may wish to consider having these officials obtain statements of attainment against appropriate units of competency in accordance with the Public Sector Training Package or undertake other appropriate training.

Part 8 – Third party arrangements

59. Entities are encouraged to make third-party providers aware of the Commonwealth's position on fraud and put measures in place to ensure that third party service providers meet the high standard of accountability required as part of the Commonwealth's financial management framework. When engaging external providers, the purchasing entity retains its fraud control responsibilities for services delivered by the third parties. When engaging another Commonwealth entity, it is important to determine which entity will be responsible for fraud control arrangements.

60. If allegations are made in relation to third-party providers, entities will need to determine whether, if proven, the fraud constitutes fraud against the Commonwealth. If a private sector contractor or non-government organisation experiences internal fraud, this does not necessarily constitute fraud against the Commonwealth. The victim of the fraud may be the contractor and any proceedings may fall under state or territory law. However, contractors and service providers may be subject to the abuse of public office offence under section 142.2 of the Criminal Code.

Part 9 – Detection, investigation and response

61. Fraud detection, investigation and response are key elements of the overall fraud control framework. Paragraphs (d) and (e) of the Fraud Rule require entities to have appropriate mechanisms for detecting and investigating fraud. The Fraud Policy requires NCEs to have detection and investigation systems consistent with the AGIS. This is to ensure the integrity of their investigations. For this reason, CCEs are strongly encouraged to follow this requirement.

Detection

62. Early detection of fraud is an essential element of fraud control. While reporting of fraud is a common means of detection, entities are encouraged to use other measures such as monitoring high-risk areas, internal reviews and audits, intrusion detection systems, conducting reviews focused on risk, or data mining and data matching.

63. Under paragraph (d) of the Fraud Rule, officials, clients and members of the public must be provided with an appropriate channel to report suspected fraud confidentially. Officials and contractors who make public interest disclosures are also entitled to protections under the *Public Interest Disclosure Act 2013*. It is important for entities to appropriately publicise these mechanisms. Entities are encouraged to establish policies and procedures to encourage and support reporting of suspected fraud

through proper channels. This can include measures to protect those making such reports from adverse consequences.

Fraud incident management protocols

64. Entities are responsible for making decisions at a number of critical stages in the management of a suspected fraud. This includes the decision to initiate an investigation (including the transition from audit or compliance work to a fraud investigation) or to refer the matter to the AFP or other law enforcement agencies. It also includes subsequent decisions on the actions resulting from an investigation, such as referral of a brief of evidence to the CDPP, or application of administrative, disciplinary or civil sanction or other action (such as a decision to take no further action).

65. The Fraud Policy requires NCEs to have appropriately documented procedures and criteria for making decisions. This is to maintain accountability and consistency in decision making at critical stages of responding to a fraud incident. For this reason, CCEs are strongly encouraged to follow this requirement.

66. Criteria for responding to a fraud incident will ideally reflect an entity's particular circumstances. It is important for criteria to go beyond the immediate financial cost of the fraud in determining the response to include factors such as deterrence and security implications.

Criteria for determining fraud response

Criteria entities may take into account in determining how to respond to fraud may include:

- financial impact
- links to terrorism or organised crime
- national security matters
- real threat to life or personal safety
- impacts on multiple entities
- impacts on industry
- political sensitivity
- corruption by a public official
- public interest
- deterrence
- policy impact, and
- integrity damage.

67. Entities are encouraged to take a common sense approach to non-compliance, misconduct and trivial fraud by having graduated and proportionate responses based on their risk tolerance and risk environment. If the evidence cannot establish the intention or conduct required for a criminal offence, it may be appropriate to apply administrative or civil sanctions. When a matter involves an official within the entity it may constitute misconduct, corruption and/or fraud. While a matter can be dealt with

as both misconduct and fraud, it is important that any misconduct proceedings are managed to avoid prejudicing criminal prosecutions.

68. Some matters of fraud may be vexatious or so trivial as to not warrant investigation and can be appropriately dealt with at the manager level. However, it is important for officials to record their response to an incident and reasons for any actions taken.

69. The Fraud Policy requires NCEs to appropriately document decisions to use civil, administrative or disciplinary procedures or to take no further action, so that matters are resolved in a consistent and defensible manner. This is to maintain accountability. For this reason CCEs are strongly encouraged to follow this requirement. Procedures can reflect the assumption that allegations of fraud will be investigated and appropriately acted upon.

70. Entities are encouraged to have in place a formal system for securely storing, recording, analysing and monitoring all instances or allegations of internal or external fraud or attempted fraud within the entity and any subsequent investigations and outcomes. Appropriately storing and reporting information on fraud matters provides better visibility for entities and the Commonwealth on fraud risks and trends.

Referrals to law enforcement agencies

71. Entities are responsible for investigating instances of fraud that are not serious or complex,[5] including investigating disciplinary matters. Entities are encouraged to seek guidance from the AFP whether a matter is serious or complex, or warrants a criminal investigation. Entities may discuss possible referrals with the AFP if there is any doubt about whether it is appropriate to refer a particular matter. Entities may outsource these investigations.

72. The AFP has the primary law enforcement responsibility for investigating serious or complex fraud against the Commonwealth. The Fraud Policy requires NCEs to refer all instances of potential serious or complex fraud to the AFP in accordance with the AGIS and the referral process published on the AFP website available at www.afp.gov.au. This applies except when legislation sets out specific alternative arrangements, or when entities have the capacity and the appropriate skills and resources needed to investigate criminal matters and meet the requirements of the CDPP in preparing briefs of evidence. This exception does not preclude an entity from referring a serious or complex matter to the AFP when deemed appropriate. CCEs are strongly encouraged to follow this requirement. The AFP can also investigate matters that could involve a real or perceived conflict of interest if they were to be investigated by the entity concerned. It is important for serious or complex fraud referrals to the AFP to be accompanied with relevant documentation and a quantification of the fraud. Relevant documentation can include:
    - an evidence matrix detailing offences considered against which persons of interest, and evidence gathered to prove physical and/or fault elements, and
    - a quantification of the fraud together with material outlining the basis as to how the referring entity calculated the quantum of the alleged fraud.

[5] Further guidance on matters that may constitute serious or complex fraud are set out in the box at the end of this Part.

73. Matters of a politically sensitive nature, deemed by the entity as appropriate for referral to the AFP can be brought to the attention of the Minister for Justice through the relevant Minister or department at the time of referral unless bringing the matter to the attention of a Minister would compromise the investigation. This enables the government to be informed at the earliest juncture of potential politically contentious matters that may require AFP investigation. The procedure exists only to enable the Minister to be informed of significant matters affecting their responsibility for the AFP. The Minister does not have the power or function of deciding what particular allegations the AFP will investigate. The decision to seek an AFP investigation will, unless the matter affects other portfolios, remain that of the complainant entity.

74. When a matter involves offences under state or territory law, entities can refer it to the responsible state or territory police service for investigation. If a matter involves cartel conduct, the entity can refer it to the ACCC, which is responsible for enforcing compliance with Australia's competition laws. Further information is available at www.accc.gov.au.

75. The AFP evaluates matters referred to it for investigation in accordance with its CCPM. The CCPM provides entities with a basis for considering matters prior to referral. The AFP and the state or territory police services may not be able to accept all referrals. If a referral is declined, the entity which made the referral is responsible for resolving the matter. The Fraud Policy requires NCEs to resolve the matter in accordance with internal and external requirements such as the AGIS and entity specific criteria. Corporate entities are strongly encouraged to follow this requirement.

76. If the AFP declines to investigate a matter, it will advise the entity of the reasons in writing at the earliest opportunity within 28 days (unless another period is agreed to). The AFP may also suggest alternative methods of handling the matter and may assist entities by executing search warrants and providing other forms of assistance. If, after the AFP has advised an entity that it cannot accept a referral, additional information becomes available that shows that the matter is more serious than first indicated, the entity may again refer the matter to the AFP for consideration.

77. An entity that needs specific arrangements with the AFP to meet its obligations and responsibilities may negotiate a service agreement with the AFP. In circumstances where there is a Commonwealth law enforcement interest, and where both parties support an out posting, the AFP may outpost officers to an entity.

Serious and complex matters referred to the AFP for investigation

To ensure that AFP resources are directed towards the matters of highest priority, the AFP evaluates all matters that are referred to it for investigation in accordance with the CCPM. The CCPM is used to assess:

- the incident type and the impact of the matter on Australian society
- the importance of the matter to both the entity and the AFP in terms of the roles assigned to them by government and ministerial direction
- the type of response required (that is, whether an immediate response is needed), and
- the resources required by the AFP to undertake the matter.

It is not possible to provide a definitive list of the types of fraud matters that will be accepted by the AFP for investigation. However, the criteria set out below provide guidance as to whether a particular matter is of sufficient seriousness and may warrant referral to the AFP:

- significant or potentially significant monetary or property loss to the Commonwealth
- damage to the security, standing or integrity of the Commonwealth or an entity
- harm to the economy, national security, resources, assets, environment or wellbeing of Australia
- a serious breach of trust by a Commonwealth official or contractor of an entity
- the use of sophisticated techniques or technology to avoid detection, which requires specialised skills and technology for the matter to be successfully investigated
- the elements of a criminal conspiracy
- bribery, corruption or attempted bribery or corruption of a Commonwealth official or contractor of an entity
- known or suspected criminal activity against more than one entity
- activities that could affect wider aspects of Commonwealth law enforcement (e.g. illegal immigration or money laundering), and
- politically sensitive matters.

Investigation

78. The investigation of fraud is crucial to effective fraud control. Conducting proper investigations is necessary to ensure the integrity of evidence and fairness for the accused. It is important for entities to maintain proper process for all investigations. An administrative investigation into a fraud matter which appears to be minor may reveal a larger fraud warranting a criminal investigation.

79. When an investigation concerns matters that are security classified, entities can refer to the Protective Security Policy Framework for information on the necessary security arrangements required for such investigations.

80. There are several key acts and policies which set out requirements and limitations for entities when conducting investigations, including the Crimes Act, the *Freedom of*

Information Act 1982, *Privacy Act 1988*, *Archives Act 1983*, Prosecution Policy of the Commonwealth and the Protective Security Policy Framework.

81. If an investigation identifies criminal activity involving another entity's activities or programs, it is important the investigating entity share this information with the other entity affected subject to any legislative provisions regulating the disclosure or use of information. While the Privacy Act places some limitations on the sharing of information, there are several exceptions which in certain circumstances allow information to be collected and shared relating to fraud investigations.

82. Investigations may put staff at risk. It is important that entities have appropriate protocols and training in place to ensure the safety of officials conducting investigations.

Prosecution and referral to the CDPP

83. Entities are encouraged to consider prosecution in appropriate circumstances. The Commonwealth's policy on prosecution of criminal offences is set out in the Prosecution Policy of the Commonwealth. Prosecutions are important in deterring fraud and in educating officers and the public generally about the seriousness of fraud. When referring matters to the CDPP for consideration of prosecution action entities are encouraged to prepare briefs in accordance with the Guidelines for dealings between Commonwealth investigators and the Commonwealth Director of Public Prosecutions.

84. If any entity needs specific arrangements with the CDPP to meet its obligations and responsibilities, in addition to those outlined in this guide, the entity and the CDPP may negotiate separate measures, such as a memorandum of understanding.

85. If an entity sends a brief of evidence to the CDPP to consider prosecution action, and the CDPP advises that a prosecution will not proceed, the entity remains responsible for resolving the matter appropriately using other available remedies. Entities are encouraged to consider civil, administrative or disciplinary proceedings for which a lower standard of proof is required. Entities can develop an enforcement strategy to ensure appropriate use of the remedies.

86. It is important for entities to take all reasonable measures to recovering financial losses from fraud through proceeds of crime and civil recovery processes or administrative remedies. Entities are encouraged to have arrangements about determining recovery action. In determining action, it is important that entities consider, in addition to the financial cost of the recovery, the deterrent value and other non-financial benefits such as public interest and integrity of the government's or the entity's reputation.

Part 10 – Quality assurance and reviews

87. Entities are encouraged to ensure appropriate monitoring and evaluation of fraud control plans by an appropriate committee or body. Compliance with the Fraud Rule (and Fraud Policy for NCEs) may be the subject of audit by the ANAO.

88. As described under the AGIS, the AFP may conduct quality assurance reviews of entity fraud investigations. The AFP will provide the results of any such reviews to AGD.

89. Entities conducting multiple investigations deemed to represent a significant risk are strongly encouraged to have a quality assurance review system in place that complements the AFP's quality assurance review process and that provides adequate information for effective monitoring and continuous improvement.

Part 11 – Reporting

90. Reporting systems that records allegations of fraud, subsequent investigation action and the outcomes can provide an overview of the nature, extent and location of fraud. They can also form the basis for developing an intelligence capability and fraud risk profiles.

91. The Fraud Rule requires entities to have systems in place to manage information gathered about fraud against the entities. Mechanisms for recording and reporting incidents of fraud can cover the number of cases and complexity of investigations undertaken, and include the outcomes of the incidents and investigations.

92. Data collection on fraud and fraud control activities is an important part of controlling fraud against the Commonwealth. The Australian Institute of Criminology, in consultation with AGD, provides an annual report on fraud against the Commonwealth and fraud control arrangements and compliance in entities.

93. The Fraud Policy requires NCEs to collect information on fraud and provide it to the AIC by 30 September each year. Corporate entities are strongly encouraged to follow this requirement. This requirement facilitates the process of annual reporting to government. Required information may include incidents of suspected fraud, incidents under investigation, completed incidents, whether the fraud was proved or not, and whether the incident was dealt with by a criminal, civil or administrative remedy.

Reporting significant issues to the responsible Minister

94. While there is no specific mention of reporting fraud matters to an entity's minister in the Fraud Rule or Fraud Policy, section 19 of the PGPA Act requires an accountable authority to keep their minister informed about the activities of the entity and significant issues that may affect the entity. This can include:
    - fraud initiatives undertaken by the entity in the reporting period, including an evaluation of their effectiveness
    - planned fraud initiatives not yet in place
    - information regarding significant fraud risks for the entity, and
    - significant fraud incidents which occurred during the reporting period.

95. Significant fraud matters can also be reported to the Minister for Finance, when they involve significant non-compliance with the finance law. When significant non-compliance with the finance law occurs, section 19 requires these matters to be reported to the Minister for Finance in addition to the responsible Minister. These reports can be copied to the Minister for Finance when they are reported to the

responsible Minister. Further guidance on reporting significant non-compliance can be found in *Resource Management Guide No.214, Notification of significant non-compliance with the finance law (PGPA Act, section 19)*. Examples of fraud matters that are likely to constitute significant non-compliance with the finance law include:

- fraud by an official (excluding trivial fraud)
- fraud involving a systematic failure of internal controls
- fraud resulting from a systematic failure in policy or program design, and
- fraud matters which are inappropriately responded to (for example, failing to have a serious fraud investigated).

96. Reporting requirements under section 19 are in place to ensure that Ministers are informed of matters relevant to their duties. In reporting a matter to a Minister, it is important for entities to use their judgement and consult the Minister's office on what matters their Minister is to be notified about. For example not all fraud matters are significant enough to warrant reporting to the Minister. Entities are also encouraged to consider the appropriateness of the timeframe for notifying the Minister. Depending on the nature of the matter, some significant issues necessitate immediate notification whereas other notifications may be more appropriately grouped together and notified according to a schedule agreed with the responsible Minister.

Annual Reporting

97. Section 17AG of the PGPA Rule contains requirements for NCEs to report on fraud control in their annual reports. The requirements include:
    - reporting information on compliance with the Fraud Rule, and
    - the accountable authority to certify that:
        - fraud risk assessments and fraud control plans have been prepared for the entity
        - appropriate mechanisms for preventing, detecting incidents of, investigating or otherwise dealing with, and recording or reporting fraud that meet the specific needs of the entity are in place for the entity, and
        - all reasonable measures have been taken to deal appropriately with fraud relating to the entity.