Australian Government

Department of Employment and Workplace Relations

Fraud and Corruption Control Strategy

2024-2026

Contents

Acting Secretary Statement

The Department of Employment and Workplace Relations (the department) supports people to have safe, secure, and well-paid work with the skills for a sustainable future. We work with State and Territory governments, other Australian Government entities and a range of service providers to provide high quality advice and services. The department is responsible for the administration of important programs, including those that deliver payments to Australians. The department also holds sensitive information. These factors could make the department a target for malicious actors and expose the Commonwealth to fraud and corruption risk.

This Fraud and Corruption Control Strategy clearly outlines how the department protects public money and data, and supports the department and its stakeholders to prevent, protect and respond to fraud and corruption. The Strategy outlines, at a high level, how the department does so and contributes to ensuring compliance with section 10 of the _Public Governance, Performance and Accountability Rule 2014_ (Ch) (PGPA Rule) and the Commonwealth Fraud and Corruption Control Framework.

The department is committed to ensuring it upholds the highest standards of integrity. Fraud and corruption against the Commonwealth affects everyone. Fraud and corruption re-directs valuable resources that could be used to achieve public good and undermines confidence in government. Everyone in the department have a crucial role to play in reducing our exposure. All workers must report suspected fraud and corruption, and all our stakeholders are encouraged to report suspected fraud and corruption via the mechanisms set out in this Strategy.

Tania Rishniw

A/g Secretary

July 2024

Introduction

The department acknowledges it cannot avoid or prevent all fraud or corruption risk. It does not tolerate dishonest, fraudulent or corrupt behaviour. This means the department will take all reasonable measures to prevent, detect and respond to fraud and corruption relating to the department and will:

- promote awareness of fraud, corruption and integrity to its workers
- assess and, where appropriate, investigate all allegations of fraud and corruption
- seek to recover losses through proceeds of crime and administrative recovery processes and
- take appropriate criminal, civil, administrative, or disciplinary action, including prosecution and termination of employment or contracts.

Definitions

Fraud

Fraud is defined in the Commonwealth Fraud and Corruption Control Framework as 'dishonestly obtaining (including attempting to obtain) a gain or benefit, or causing a loss or risk of loss, by deception or other means'. The conduct does not need to represent a breach of criminal law. A benefit or loss is not restricted to a material benefit or loss and may be tangible or intangible. A benefit may also be obtained by a third party.

Internal fraud

Internal Fraud is a form of corruption that is committed by departmental workers and can include:

- falsely claiming employee entitlements
- unauthorised access, modification, theft, or disclosure of information
- misdirection or theft of department funds or
- use or theft of department assets for personal or third-party benefit.

External fraud

External fraud is that committed by parties external to the department such as service providers, recipients of the department's services or members of the public and can include:

- submitting false information to receive subsidies, payments, services, or other benefits
- applying for loans or other support payments using false or stolen identities
- unauthorised access, modification, theft, or disclosure of information
- deliberately omitting information when interacting with the department's programs or
- submitting false invoices or invoices for work not completed.

Corruption

Corruption is defined in the Commonwealth Fraud and Corruption Control Framework, consistent with the _National Anti-Corruption Commission Act 2022_ (NACC Act), as 'any conduct that does or could compromise the integrity, accountability, or probity of public administration'. Corruption may be criminal or non-criminal in nature and may affect any aspect of public administration. This includes:

- Any conduct of any person (whether or not a staff member of a Commonwealth agency[1]) that adversely affects, or that could adversely affect, either directly or indirectly
    - the honest or impartial exercise of any staff member's powers as a staff member of a Commonwealth agency or
    - the honest or impartial performance of any public official's functions or duties as a public official.

---

[1] A staff member of a Commonwealth Agency has the same meaning in relation to the entity as defined in the NACC Act 2022 and includes APS staff, contractors, and contracted service providers.

- Any conduct of a staff member of a Commonwealth agency that constitutes or involves a breach of public trust.
- Any conduct of a staff member of a Commonwealth agency that constitutes, involves, or is engaged in for the purpose of abuse of the person's office.
- Any conduct of a staff member of a Commonwealth agency, or a former staff member of a Commonwealth agency, that constitutes or involves the misuse of information, or documents acquired in the person's capacity as a staff member of a Commonwealth agency.

The following examples list behaviour that may amount to corruption:

- collusion between APS staff and a potential contractor
- bribery (domestic or foreign)
- obtaining, offering, or soliciting secret commissions, kickbacks, or gratuities
- one or more individuals manipulating a procurement process for personal gain
- nepotism, or preferential treatment of family members
- cronyism, or preferential treatment of friends and associates
- acting (or failing to act) on a conflict of interest (CoI)
- unlawful disclosure of official or commercially sensitive information or
- insider trading, or misusing official information to gain an unfair private, commercial or market advantage for self or others.

Non-compliance

Non-compliance is any failure to meet obligations under applicable laws, regulations, agreements, contracts, or other requirements. This includes intentional, reckless, negligent and unintentional acts.

As fraud or corruption typically require intent, actions resulting from carelessness, accident or error are generally considered non-compliance. Non-compliance can evolve into sharp practice (behaviour that is not illegal but is morally or ethically wrong) or fraud and corruption, especially when deception is involved. Effective management of non-compliance is an essential element of controlling fraud and corruption risks.

Unethical Behaviour

The APS Values and Code of Conduct describe the behaviour expected of public officials which includes acting with honesty, diligence, avoiding conflicts of interest, and ensuring the proper use of information. The department has formal procedures for investigating potential breaches of the APS Values or Code of Conduct.

Governance

Fraud and Corruption Control Framework

The department's Fraud and Corruption Control Framework is consistent with the Commonwealth Fraud and Corruption Control Framework. It includes governance, risk management, policies and procedures and is implemented with the Prevent, Detect, Respond model.

Key Roles and Responsibilities

Role	Responsibility
Secretary	As the Accountable Authority under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), the Secretary is responsible for taking all reasonable measures to prevent, detect and respond to fraud and corruption relating to the department. The Secretary must refer suspected serious or systemic corrupt conduct by current or former departmental officials to the NACC.
Chief Security Officer	Provides strategic oversight and management of security across the department.
Chief Information Security Officers	Facilitate communications between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives; provides strategic-level guidance for the agency security program and ensures compliance with national policy, standards, regulations, and legislation.
Chief Risk Officer	Ensures the department's risk management approach facilitates the efficient and effective governance of significant risks, including those involving fraud and corruption.
Deputy Secretaries	Provide oversight of fraud and corruption management in their Group and ensure effective application of all reasonable fraud and corruption controls.
First Assistant Secretaries	Oversee the assessment and management of fraud and corruption risks relevant to their Division including prevention, detection, and response where appropriate. Ensure detailed fraud and corruption risk assessments for functions within their Division are conducted in accordance with the department's Fraud and Corruption Control Policy. Ensure fraud and corruption risks shared across agencies or business functions are understood and appropriately managed.
Assistant Secretaries	Oversee management of fraud and corruption risks for their Branches including ensuring that fraud and corruption risks are understood and appropriately documented and controlled.
Audit and Risk Committee (ARC)	Consistent with section 17 of the PGPA Rule, provide independent advice to the Accountable Authority about financial reporting, performance reporting, system of risk oversight and management, and systems of internal control. This includes the risk oversight and management of systems in place to manage the department's fraud and corruption risks.
Enterprise Risk, Assurance and Investigations Branch	Responsible for coordinating the department's implementation of the Commonwealth Fraud and Corruption Control Framework.
People Branch	Responsible for coordinating the department's implementation of the APS Values and Code of Conduct in practice; conducting code of conduct investigations ; and referring conduct that could be considered corruption to Enterprise Risk, Assurance and Investigations Branch.

Role	Responsibility
Finance Branch	Responsible for the department's Procurement, Gifts and Benefits, and Travel and Credit Card policies, monitors and reports identified financial non-compliance and manages the annual Management Assurance Certificate issued to SES.
Risk Committee	The Risk Committee supports the Secretary, the Executive Board and the Audit and Risk Committee by providing oversight of the effectiveness and appropriateness of the department's risk management arrangements and supporting system; and a forum to support and promote a positive risk and security culture within the department.
Public Interest Disclosure Officers	As per the _Public Interest Disclosure Act 2013_, must refer suspected serious or systemic corrupt conduct involving current or former departmental officials to the NACC.
Managers	Foster a culture of integrity in their business areas together with the implementation and operation of governance arrangements including: - ensuring fraud and corruption risks are considered when planning and conducting business - ensuring staff understand and comply with relevant legislation, regulations, procedures, and policies and - assisting relevant officials to conduct fraud and corruption control activities, including risk assessments.
Public officials, including staff, contractors, and contracted service or third-party providers	Act with honesty and integrity and comply with legislated and policy requirements. Report all suspected instances of fraud or corruption. Cooperate with the department and NACC as public officials.
Recipients of the department's services, payments, or assistance	Provide the department and its service providers accurate and timely information. Report all suspected instances of fraud or corruption.

Fraud and Corruption Reporting

Reporting and monitoring provides assurance regarding the effectiveness of the department's control arrangements to prevent, detect and respond to fraud and corruption. The department collects information on all allegations of fraud and corruption against the department, all current and completed investigations and the outcome of the assessment or investigation. The department's reporting, assurance and monitoring controls include:

Fraud certification and annual report
Each year, the Secretary certifies in the annual report whether the department has met the requirements of the Fraud and Corruption Rule, in accordance with section 17AG of the PGPA Rule.

Reporting to governance committees
The department's key fraud and corruption control initiatives, integrity initiatives and investigation updates are regularly reported to the ARC and the Risk Committee.

Annual reporting to the Australian Institute of Criminology

Per the Commonwealth Fraud and Corruption Control Framework, the department collects data on risks and instances of fraud and corruption and reports this information annually to the Australian Institute of Criminology.

Enterprise Fraud and Corruption Risks

The department conducts an Enterprise Fraud and Corruption Risk Assessment at least every 2 years, in accordance with the Commonwealth Fraud and Corruption Control Framework. The department's enterprise fraud and corruption risks are as follows:

Information

The department controls and has access to large volumes of official business information that is potentially personal, sensitive, security classified or otherwise requires protection. Official business information is an attractive target for acts of fraud or corruption and can attract motivated and sophisticated external parties, including organised crime.

The department also receives a large volume of information that informs decisions relevant to fraud and corruption targets. This includes information relevant to awarding and continuing contracts; promotions and entitlements; entry to programs; or approval of loans, payments, subsidies or grants. This makes the department vulnerable to receiving false information.

Risk events include theft, misuse, unauthorised access and modification or disclosure of intellectual property or official business information.

The department needs to be on the lookout for receiving and acting on false information.

Finance

The department is responsible for management of a multi-billion-dollar budget, which presents an attractive target for potential acts of fraud or corruption. The department's operations involve payments and procurements, including those regarding salaries, contracts, grants, loans and subsidies.

Possible risk events include theft, misuse or misdirection of: payroll, entitlements, cash, credit cards, reimbursements, invoices, revenue, grants, subsidies and loans.

Outcomes of decisions

The department and its officials are responsible for decisions that result in benefits, including non-financial benefit. These can include decisions to allow entry into a program, those regarding loan forgiveness or decisions about the application of compliance responses.

Possible risk events include misuse of power or position, acting on inducement such as bribery or coercion and making decisions with dishonest intent to cause benefit or loss.

People

The department is staffed by highly trusted officials, with opportunities to commit or be a party to acts of fraud or corruption. Staff also have the potential for conflicting interests across a range of domains. While a conflict of interest is not inherently corrupt, failure to identify and manage conflicts appropriately can expose the department to increased corruption risk. The appropriate management of conflict of interest also applies to Financial Risks.

Possible risk events include bias in recruitment processes, undeclared or mismanaged conflicts of interests and inducements being provided to decision-makers to influence outcomes.

Assets and systems

The department owns and/or is responsible for a range of assets including ICT equipment and systems, vehicles, furniture and facilities. These assets can have monetary value if sold and have personal or intrinsic value if stolen or misused and are common targets for acts of fraud or corruption.

Possible risk events include theft, damage or misuse of any department-controlled assets, including IT systems, facilities, vehicles, equipment, and other tangible, intangible or physical assets.

Fraud and Corruption Controls

Prevent

Fraud and corruption prevention initiatives focus on establishing and maintaining sound governance systems, systems of control and an ethical organisational culture. Prevention strategies are the most effective way to mitigate fraud and corruption and operate by reducing the likelihood and impact of fraud and corruption events. The department's prevention strategies include:

- fraud and corruption, security, and integrity awareness training
- conflict of interest management, including declarations and guidance
- a robust system of internal controls implemented at the program, policy, business function and project levels
- a comprehensive information security framework
- fraud and corruption risk management integrated into enterprise risk management arrangements and
- implementing the Protective Security Policy Framework and workforce screening controls.

Detect

Effective systems are necessary to detect fraud and corruption quickly to minimise impact. Measures to detect fraud and corruption within the department include:

- fraud and corruption reporting channels including email, phone and anonymous options
- availability of Authorised Officers under the Public Interest Disclosure Scheme
- detective controls implemented at the business level, including compliance programs and data analytics
- participation in the Fraud Fusion Taskforce and
- an annual program of internal audits.

Respond

Response controls are a vital component of the department's fraud and corruption control framework. These aim to disrupt, discontinue and recover from fraudulent or corrupt activity and provide general deterrence. Response strategies include:

- fraud and corruption allegation assessment and investigation
- prosecution where sufficient evidence is available
- recovery of losses via civil, criminal, or administrative processes and
- post incident reports to assist in addressing known vulnerabilities.

Reporting Suspected Fraud and Corruption

Department of Employment and Workplace Relations

You can report suspected fraud or corruption to the department's Fraud Intelligence and Investigations Team by:

- Email: fraud@dewr.gov.au
- Phone: (02) 6240 8888
- Online: Whispli (anonymous reporting tool) - https://dewr-gov-au.whispli.com/reportfraud
- Post: Fraud Intelligence and Investigations Team
           PO Box 9828
           Canberra ACT 2601

Please provide as much information as possible, however do not investigate the matter yourself.

If possible, include the following information:

- Who is involved? Include the name/s of the person/s or organisation/s, address/es and phone number/s.
- What fraud or corruption do you think has occurred? Including how, when and where it occurred.
- If you believe the behaviour or issue is continuing.
- How you came to know about the matter.

Where possible, please provide supporting documentation. You do not need to provide your contact details; however, it can assist the department to assess and investigate the allegation.

If you are unsure whether an activity constitutes fraud or corruption, please contact the Fraud Intelligence and Investigations Team for advice.

Fair Entitlements Guarantee

You can also report Fair Entitlements Guarantee related fraud directly to the Fair Entitlements Guarantee Branch via the Reporting FEG related fraud website.

National Anti-Corruption Commission (NACC)

The department reports all cases of suspected serious or systemic corruption to the NACC, and complies with requests from the NACC, in accordance with the NACC Act 2022.

The NACC considers most people who work for, exercise the powers of, or perform functions for, the Australian Government or the Australian Parliament as public officials for the purpose of investigating corruption. This includes consultants, independent contractors and labour-hire contractors directly engaged by the department. It also includes external service providers and third-party providers who are required to adhere to all contractual and/or legal obligations, program guidelines or conditions of funding that govern their relationship with the department. A failure to comply with these obligations may constitute corruption or fraud.

Anyone can report serious or systemic corruption directly to the NACC. Information on how to submit reports directly, including protections that exist for those to make referrals, is available via the NACC website.

Public Interest Disclosure

The Public Interest Disclosure Act 2013 seeks to promote integrity and accountability by:

- encouraging the disclosure of information about alleged serious wrongdoing
- protecting those who make such disclosures and
- ensuring that disclosures are properly actioned.

The department will act on disclosures as appropriate, and protect disclosers from any reprisals for making a disclosure. A person must be a current or former public official, including staff of third party

contracted service providers, to report under the Public Interest Disclosure scheme.
To make a Public Interest Disclosure a person can:

- email PID@dewr.gov.au. This can include requesting contact directly from a departmental Authorised Officer or
- disclose to their supervisor.

Further information on public interest disclosures at the department can be found on the Department's website.

Privacy

Those who report suspected wrongdoing, fraud or corruption to the department are protected by law, including the *Privacy Act 1988*, and their personal information is collected by the department for the purposes of assessing allegations of suspected wrongdoing, fraud, or corruption. The department may disclose the personal information provided to other Commonwealth, State or Territory bodies (including law enforcement bodies) for appropriate assessment or action. Personal information may also be used by the department or given to other parties if it is required or authorised by law. Your personal information is unlikely to be disclosed overseas.

For more information about how the department manages personal information (including information on accessing or correcting your personal information) and how to make a privacy complaint, please view our full privacy policy or you can request a copy from the department by sending an email to privacy@dewr.gov.au.

Further Information

For further information about this document, the Fraud and Corruption Control Framework, PID or Integrity matters contact Integrity@dewr.gov.au

For information about reporting suspected fraud and corruption, fraud intelligence and investigations contact Fraud@dewr.gov.au

For further information see:

Commonwealth Fraud and Corruption Control Framework 2024

DEWR Privacy Policy

Australian Government Investigations Standards

APS Values and Code of Conduct in Practice

Public Governance, Performance and Accountability Act 2013 (PGPA Act)

PGPA Rule 2014

Privacy Act 1988

Public Interest Disclosure Act 2013

Proceeds of Crime Act 2002

Public Service Act 1999

Criminal Code Act 1995 (Commonwealth)

National Anti-Corruption Commission Act 2022

Protective Security Policy Framework

Document Details

Owner	Enterprise Risk, Assurance and Investigations Branch
Document Status	Final
Point of Contact	Director, Integrity
Approver	Deborah Jenkins
Approval Authority	Chief Operating Officer
	Department of Employment and Workplace Relations
Date of Approval	12 June 2024
Version Control	Version 1.1

Version History

Version	Description	Approver	Date
1.0	Original	Deborah Jenkins	12 June 2024
1.1	Fraud hotline number update	Integrity Team	13 August 2024