
Issued by: Anthony Li Chiang
Contact: Anthony Li Chiang
Release Date: 14/01/2019
Version: 1.0

Document Location: Fraud Control Plans\Industry FCP 2018-20v1.2
## CONTENTS

1. Forward from the Secretary ........................................... 5
2. Introduction .................................................................. 6
3. Fraud and Corruption Statement .................................... 6
4. Code of Conduct .......................................................... 6
5. Definition of Fraud ......................................................... 7
   5.1 Definition of Corruption ............................................. 7
   5.2 Conflict of Interest ..................................................... 7
   5.3 Foreign Bribery and Foreign Influence Transparency Scheme 8
   5.4 Insider Threat .......................................................... 8
   5.5 Cyber and Digital Awareness ...................................... 9
   5.6 Contact Reporting ..................................................... 9
6. Internal Control System .................................................. 10
7. Fraud Control Framework ................................................. 10
   7.1 Governance ............................................................. 11
   7.2 Executive Board ....................................................... 11
   7.3 People Committee ..................................................... 11
   7.4 Programme Assurance Committee .............................. 11
   7.5 ICT & Data Strategy Committee ................................. 12
   7.6 Assurance and Audit Committee ................................. 12
   7.7 Fraud Prevention ...................................................... 12
   7.8 Fraud Detection ....................................................... 12
   7.9 Fraud Response ....................................................... 12
   7.10 Fraud Monitoring, Evaluation and Reporting ................ 12
   7.11 Fraud and Corruption Strategy and Action Plan .......... 13
8. Fraud Control Policy and Principles ................................. 13
9. Fraud Roles, Responsibilities and Accountabilities ............... 13
   9.1 Overall Responsibility for Fraud Control ..................... 13
   9.2 Authorised Official - Fraud Control Officer (FCO) .......... 13
10. How to Report Fraud and Other Suspicious Activity .......... 14
    10.1 Fraud Reports from Internal Parties ......................... 14
    10.2 Fraud Reports from External Parties ......................... 14
    10.3 Fraud Advice ....................................................... 14
    10.4 Reporting Other Unusual and Suspicious Activity ....... 15
    10.5 What to Expect When You Report Fraud ................. 15
    10.6 Protection of Employees Reporting Suspected Fraud .... 15
    10.7 Public Interest Disclosure ....................................... 15
    10.8 Anonymity .......................................................... 15
    10.9 Privacy .............................................................. 15
11. Fraud Investigations .................................................... 16
    11.1 The Role of the Australian Federal Police (AFP) .......... 16
    11.2 The role of the Commonwealth Director of Public Prosecutions (CDPP) 16
12. Risk Management 16
   12.1 Fraud Risk Assessment Process 16
   12.2 Risk Management Framework 17
13. Fraud Prevention Strategies 18
   13.1 Fraud Awareness Training 18
   13.2 Employment Screening 18
   13.3 Leave Policies 18
   13.4 Declaration of Interest and Conflict of Interest Policy 18
   13.5 ICT Security 18
14. Fraud Detection Strategies 18
   14.1 Fraud Reporting Mechanisms 18
   14.2 Internal Audit 19
   14.3 Security 19
   14.4 Compliance Reviews 19
   14.5 ICT Compliance 19
15. Fraud Response Strategies 19
   15.1 Investigation Resources 19
   15.2 External Investigation Resources 19
   15.3 AFP Referrals 20
   15.4 Disciplinary Procedures 20
   15.5 Policy for Civil Proceedings to Recover the Proceeds of Fraud 20
16. Fraud Monitoring Reporting and Evaluation Strategies 20
   16.1 Insurance 21
   16.2 Fraud Control Reporting Requirements 21
Attachment A Frequently Asked Questions 22
Forward from the Secretary

Welcome to the Fraud and Corruption Control Plan 2018-20.

The Department of Industry, Innovation and Science (the department) takes our exposure to fraud seriously and has a zero tolerance for it occurring. The department takes all reasonable measures to control fraud and properly manage public resources in a way that assures the integrity of the activities of the department while maximising benefits for the Australian people.

Fraud is a threat which affects every Commonwealth entity in all areas of business, including benefits, taxation, procurement, grants and internal procedures. Fraud against the Commonwealth is a criminal offence that impacts all Australians. It reduces funds available for delivering public goods and services, can place public safety at risk and undermines public confidence in government.

This department is central to the achieving the Government’s vision for the growth and productivity of globally competitive industries. Every day we work closely with industry, businesses, the science community and other stakeholders to help build and drive economic growth. We must remain constantly vigilant of fraud vulnerabilities across all our programs and activities and ensure robust controls are in place. Through sound administration, we play a critical role in safeguarding the Commonwealth against fraud.

We should also be aware of threats from within. The ‘trusted insider’ represents a real and enduring risk to everyday business practices. A trusted insider is someone who leaks information or takes material outside of our organisation without authorisation, to gain benefit or cause a loss. Insider activity undermines the integrity and reputation of our organisation, and can also be a threat to both our economic and national security.

To ensure we meet our obligations under the Public Governance Performance and Accountability Act 2013 and the Commonwealth Fraud Control Framework 2017, the department has developed this ‘Fraud and Corruption Control Plan 2018-20’ (FCCP). The FCCP ensures that the department establishes and maintains appropriate systems of risk oversight and management, and that all reasonable measures are in place to prevent, detect and deal with fraud.

All staff and contractors have a role in the department’s fraud control arrangements, including identifying and reducing fraud risks, reporting suspected fraud and participating in fraud control activities. As APS employees, we are committed to the highest ethical standards as embedded in the APS Values, Employment Principles, and Code of Conduct.

Dr Heather Smith
Secretary
Department of Industry, Innovation and Science
2. Introduction

The Fraud and Corruption Control Plan (FCCP) documents the strategic and operational approach to controlling fraud and corruption within the Department of Industry, Innovation and Science (the department). It provides an overview of how fraud and corruption risks will be managed and complies with the requirements of the Commonwealth Fraud Control Framework 2017 (the Framework).

This FCCP has been prepared in accordance with the department’s obligations pursuant to the Framework which sits under the Public Governance, Performance and Accountability Act 2013 (PGPA Act).

The Framework outlines the Australian Government’s requirements for fraud control, including the need for government entities to put in place a comprehensive programme that covers prevention, detection, investigation and reporting strategies.

The Fraud Control Section is the internal assurance function responsible for the development and implementation of the FCCP.

This FCCP represents the department’s commitment to fraud control, and aims to minimise the potential for fraud enacted on the department’s programmes or activities by employees or people outside the department.

3. Fraud and Corruption Statement

The department is committed to reducing fraud and corruption risk by complying with the requirements of the Framework through:

- a Fraud and Corruption Control Plan
- training employees in ethics, privacy, fraud and corruption awareness
- working to prevent, detect, disrupt and investigate fraud and corruption, and to achieve deterrence to fraud against the department, including by prosecuting offenders in appropriate circumstances
- applying, civil, administrative or disciplinary penalties and sanctions where appropriate
- recovering proceeds of fraudulent and corrupt activity
- a rolling programme of fraud and corruption related risk assessments
- implementing an integrated system of appropriate and effect controls
- providing specialised training for employees involved in fraud and corruption control activities
- reporting all fraud to Government.

The department recognises that breaches of the fraud rule may attract a range of criminal, civil, administrative and disciplinary remedies (reported under the PGPA Act, the Public Service Act 1999 the Criminal Code Act 1995 and the Crimes Act 1914).

4. Code of Conduct

The department’s attitude to ethical conduct is documented in the department’s Code of Conduct Policy which is based on the Australian Public Service (APS) Code of Conduct and requires all employees to meet the standards of conduct.

The Code of Conduct procedure is provided to assist in understanding the Code of Conduct and steps to be taken for alleged breaches. It also helps to identify and address issues associated with behavioural standards that are often integrally linked to performance problems.

Where an employee is found to have breached the Code of Conduct, the Secretary (or the delegate) may decide to take misconduct action. The department’s Code of Conduct Policy outlines the process to managing suspected breaches.
5. Definition of Fraud

In accordance with the Framework, fraud against the department is defined as:

“Dishonestly obtaining a benefit, or causing a loss, by deception or other means”

The Fraud Guidance sets out a range of activities which fall broadly under the definition of fraud. Fraud can be committed by staff (internal fraud) or by persons external to the department (external fraud). It may also be committed jointly between an employee and outside party. Offences of fraud against the Commonwealth may be prosecuted under a number of different Commonwealth laws.

Examples of the types of conduct that would fall within the department’s definition of fraud include (but are not limited to):

- theft
- misuse of Commonwealth credit cards
- accounting fraud (false invoices, misappropriation etc.)
- unlawful use of, or obtaining property, equipment, material or services
- causing a loss, or avoiding and/or creating a liability
- providing false or misleading information to the Commonwealth, or failing to provide it 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
- wrongfully using Commonwealth information or intellectual property.

A benefit is not restricted to monetary or material benefits, and can be either tangible or intangible, including the unauthorised provision of access to, or disclosure of information. Fraud against the Commonwealth can take many forms and may target:

- revenue (e.g. income tax, GST fraud, customs duties)
- property (e.g. cash, computers, other portable and attractive items, stationery)
- information and intelligence (e.g. personal information or classified material)
- programme funding and grants
- entitlements (e.g. expenses, leave travel, travel allowances, attendance records)
- facilities (e.g. unauthorised use of vehicles, information technology and telecommunication systems), and
- money or property held in trust or confiscated.

5.1 Definition of Corruption

AS/NZ 8001:2008 – Fraud and Corruption Control, defines corruption as:

“Dishonest activity in which a director, executive, manager, employee or contractor of an entity acts contrary to the interest of the entity and abuses his/her position of trust in order to achieve some personal gain or advantage for him or herself for another person or entity”.

The following list provides examples of types of behaviour that, if serious enough, may amount to corruption:

- bribery, domestic or foreign—obtaining, offering or soliciting secret commissions, kickbacks or gratuities
- fraud, forgery, embezzlement
- theft or misappropriation of official assets
- nepotism—preferential treatment of family members
- cronyism—preferential treatment of friends
- acting (or failing to act) in the presence of a conflict of interest
- unlawful disclosure of government information
- blackmail
- perverting the course of justice
- colluding, conspiring with, or harbouring criminals
- insider trading—misusing official information to gain an unfair private, commercial or market advantage for self or others
- green-lighting—making official decisions that improperly favour a person or company, or disadvantage another.

Complex fraud, which may also constitute corrupt conduct, can include instances where an employee or group of employees are targeted and succumb to exploitation by external parties, or initiate the misconduct.

The department must be alert to the risk of complex fraud involving collusion between agency employees and external parties.

5.2 Conflict of Interest

A conflict of interest is a circumstance which places an employee in a position where their personal interests (including those of their immediate family – to the extent known) could compromise their independence. Apparent (or perceived) conflicts of interest may be as important as actual conflicts.

The APS Code of Conduct requires APS employees to disclose and take reasonable steps to avoid any conflict of interest in connection with APS employment.

The department’s Conflict of Interest and Insider Trading policy provides a reporting framework which enables employees to disclose, and take reasonable steps to avoid, any conflicts of interest in connection with their APS employment.

---

1 Commonwealth Fraud Control Framework 2017 (the Framework)
2 Resource Management Guide No. 201 - Preventing, detecting and dealing with Fraud (Fraud Guidance)
The policy also provides guidance for all employees on how to recognise and avoid insider trading (refer section 13.4). This policy applies to all employees covered by the department’s Enterprise Agreement.

There is no standard list of items that must be disclosed. It is an employee’s responsibility to consider and disclose any personal interests or relationships that influence, or could be seen to influence, their actions. These may include:

- financial interests
- personal interests
- relationships
- outside employment
- gifts and benefits
- insider trading

Each year, all employees are required to watch the Awareness Tutorial in PageUp. The tutorial will:

- increase your awareness of conflict of interest
- provide you with an understanding of your responsibilities
- outline what steps you need to take should you have a conflict of interest to disclose

Further information is around Conflicts of Interest and the disclosure process is available in iCentral.

### 5.3 Foreign Bribery and Foreign Influence Transparency Scheme

The Australian Government Policy on foreign bribery states:

> “Australia has a zero tolerance approach to foreign bribery and corruption. Australia works actively with foreign governments to stamp out bribery, and strongly discourages companies from making facilitation payments.

The Australian Government supports ethical business practices, and the prosecution of those who engage in illegal practices. This helps to improve Australia’s investment opportunities overseas and is an important aspect of Australia’s global reputation.

Foreign bribery undermines the reputation of all Australian businesses and impacts negatively on business and government relations.”

Individuals or companies that commit the offence can be prosecuted in an Australian court. The maximum penalty for individuals found guilty of bribing a foreign public official is 10 years imprisonment and/or a fine of $1.8 million.

Should staff suspect that bribery of a foreign public official may have occurred they must notify their supervisor or the Fraud Control Officer (FCO) as soon as practicable. If you are travelling overseas and need more information or wish to discuss, please contact the FCO (refer Section 10. How to report fraud and other suspicious activity).

Lobbying Commonwealth public officials in Australia on behalf of a foreign principal for the purpose of political or government influence is now a registrable activity under the Foreign Influence Transparency Scheme which commenced on 10 December 2018.

The scheme aims to capture the nature, level and extent of foreign influence on Australia’s government and political processes and to make this more transparent.

This scheme establishes registration obligations for individuals and entities that undertake certain activities on behalf of foreign principals. Additional obligations apply to people who have previously held senior public positions in Australia. Failing to comply with obligations under the scheme may result in criminal penalties.

Staff are encouraged to contact the Attorney-General’s Department if they require further advice, or consider a person may be deliberately avoiding registration obligations.

Additional information is available on the Attorney-General’s Department website.

### 5.4 Insider Threat

Staff should be aware of the trusted insider threat. Trusted insiders are potential, current or former employees or contractors who have legitimate access to information, techniques, technology, assets or premises.

Trusted insiders can intentionally or unknowingly assist external parties in conducting activities against the organisation or can commit malicious acts for self-interest. There is no one type of trusted insider. However, there are broadly two categories of trusted insiders who pose a threat:

- The unintentional insider: unintentional insiders are trusted employees or contractors who inadvertently expose, or make vulnerable to loss or exploitation, privileged information, techniques, technology, assets or premises. Inadvertent actions include poor security practices, such as leaving IT systems unattended and failure to secure sensitive documents, and unwitting unauthorised disclosure to a third party.
- The malicious insider: malicious insiders are trusted employees and contractors who deliberately and willfully breach their duty to maintain the security of privileged information, techniques, technology, assets or premises.
Staff should be aware that due to the nature of some of the classified information they have access to that they may be a target for organised crime groups or foreign intelligence services (refer to Section 5.6. Contact Reporting).

For advice or report an Insider Threat, staff should seek advice from the Security Services team in the first instance (refer section 10 How to report fraud and other suspicious activity).

5.5 Cyber and Digital Awareness

All employees and guests of the department have a shared responsibility for ensuring good security practices. There is a critical need to protect our ICT facilities and resources, and to retain confidence of our stakeholders and clients who entrust sensitive information to the department. This includes against the risk of fraud, which is defined earlier in this Plan. These can take place in many forms, including phishing attacks; malware and viruses; identity theft; blackmail and money laundering.

The department faces numerous threat sources that can be involved in fraud including (but are not limited to):

- Nation States Foreign Intelligence Services (FIS);
- politically motivated nationalist groups;
- malicious individuals motivated by personal gain;
- hacktivists;
- insider threats and;
- organised crime

These threat sources all have numerous different attack vectors of varying complexity and success rates. These groups will record all information that they are able to retrieve, from all sources they are able to find, so that they can increase the likelihood of a successful attack on the department. To help mitigate these risks, it is recommended that staff adhere to the following controls:

- staff should be aware that all information they post online (publically and privately) is in the public domain, and could be used to attempt to socially engineer individuals;
- staff must maintain separate business and personal social media profiles;
- staff must only post departmental information online that has been approved by the department for release into the public domain;
- staff should verify requests involving expenditure are following the department’s approved processes;
- should staff believe that they have had interaction with a suspicious email or attachment, or have witnesses an attempt (failed or successful) to misuse the department’s resources, they must notify the ICT security team (refer Section 10. How to report fraud);
- additional information around the department’s social media policy is available on the intranet.

5.6 Contact Reporting

Contact reporting involves suspicious, ongoing, unusual or persistent contact with foreign officials and other foreign nationals.

Contact with foreign officials and other foreign nationals includes any type of interaction and may be work related, social or incidental. It may occur in Australia or when travelling overseas for business or leisure. For example:

- invitations to attend functions
- sport or recreation activities
- visits to embassies, consulates or involvement with trade missions
- membership to international clubs, institutes or professional associations
- incidental social interaction
- email, phone calls or online social networking sites
- training or study

The initial contact may be subtle, carefully planned or occur over an extended period of time. Staff may not even be aware that it is occurring, as the contact first attempts to gain trust and build up a relationship over a period of time before asking for bits of information or favours. Examples of suspicious contact may include, but are not limited to:

- interest in their or another employee’s official, social or personal activities
- requests for information about other people in the department or government
- a request to meet outside of the work environment
- introduction to another person with similar interests
- encouragement to participate in questionable or illegal activity
- offers of hospitality or gifts.

Staff need to report suspicious, ongoing, unusual or persistent contact with foreign officials and other foreign nationals. Human intelligence gathering is a low-risk and common method used by foreign intelligence services to gather intelligence.

Small pieces of information about your interactions with foreign officials can assist the Australian Government to develop an aggregate picture of a potential foreign intelligence service. Therefore, it is important staff recognise that an ‘innocent’ conversation or email could be part of a human intelligence gathering exercise.

In the event of a Contact, staff should seek advice from the security services team in the first instance (refer section 10. How to report fraud and other suspicious activity).
6. Internal Control System

The department has a strong system of internal controls, including our governance, risk management and policy frameworks.

These controls are operationalised by a range of security and audit functions across the department by the Divisions; ensuring that fraud and corruption risks are considered in business as usual activities.

The Assurance and Audit Committee is responsible for the oversight of the department’s fraud and corruption control arrangements and ensuring that the department has appropriate processes and systems in place to detect, capture and effectively respond to fraud and corruption.

7. Fraud Control Framework

Fraud control is further ensured not only by the implementation of Australian Government legislative requirements but by the adoption and promotion of practices recommended by the Australian National Audit Office (ANAO) and other organisations. The department has adopted the key elements recommended in the ANAO Better Practice Guide: Fraud Control in Australian Government Entities 2011 which provides an overarching approach to effective fraud control within the department. The Executive and senior management set the ‘tone at the top’ by creating an ethical culture where staff are encouraged to identify and manage potential fraud risks.

Adapted for this publication from ANAO Fraud Control in Australian Government Entities 2011
7.1 Governance
A clear and accountable corporate governance framework is vital to the department’s sound operation and performance. Governance in the public sector aims to ensure that outcomes are achieved in a way that enhances confidence in the organisation, its decisions and its actions.

7.2 Executive Board
The Executive Board provides senior leadership, strategic direction, makes key decisions (consistent with the PGPA Act) and reviews risks for the department. Its primary focus is strategic planning, performance monitoring and resource allocation. It also regularly reviews organisational health based on a range of indicators, including financial performance, internal stakeholder relationship management, human resources and ICT capability.

The Executive Board is responsible for the department’s Strategic Plan and setting the department’s risk appetite.

7.3 People Committee
The People Committee supports the Executive Board to achieve the department’s vision. The Committee is a forum, complementing direct staff engagement, Divisional Consultative Committee (DCC) and the National Consultative Committee (NCC), to surface Human Resource (HR) issues and opportunities. The Committee also provides a forum to socialise new ideas to improve performance relating to our most important asset – people.

Specifically the Committee will:
• surface HR issues
• discuss opportunities to improve implementation including members piloting initiatives, identifying risk and opportunities and ways to manage them
• champion implementation of HR initiatives and assist with their communication
• take decisions on operational HR matters
• surface strategic HR issues and convey them to Executive Board.

7.4 Programme Assurance Committee
The Programme Assurance Committee has been established to provide the Executive Board with assurance in relation to programmes within its remit.

The Programme Assurance Committee supports programme Accountable Officers and Senior Responsible Officers in driving excellence in programme design and delivery by providing an open forum for exchanging and sharing ideas. The Committee also facilitates peer learning, including risk evaluation planning for programmes.
7.5 ICT & Data Strategy Committee
The purpose of the ICT & Data Strategy Committee is to enable the department to effectively marshal its data holdings for the purposes of effective administration, monitoring, evaluation and analysis. It does this by developing ICT and staff capability to link, harness, and publish insights from our data, and by fostering a culture that champions open data and data sharing.

7.6 Assurance and Audit Committee
The Secretary has established the Assurance and Audit Committee (the Committee) in compliance with section 45 of the PGPA Act, Section 17 of the PGPA Rule and AAI 1.3.

The objective of the Committee is to provide independent assurance and assistance to the Secretary (and the Executive) on the department’s risk, control and compliance framework, and its financial statement responsibilities.

The Committees responsibilities in terms of fraud are to:
• review whether management has in place a current and comprehensive risk management framework and associated procedures, for the effective identification and management of the department’s financial and business risks, including fraud;
• review the process of developing and implementing the department’s fraud control arrangements and satisfy itself that the department has appropriate processes and systems in place to detect, capture and effectively respond to fraud related information; and
• review reports on fraud from the department’s Fraud Control Officer that outline any identified allegations of fraud, the status of any ongoing investigations and any changes to identified fraud risk in the department.

7.7 Fraud Prevention
Management, staff, consultants and contractors of the department are the first line of defence when it comes to identifying a range of risks, including fraud. The department encourages all managers and staff alike to be vigilant, and to diligently report any instance of suspected fraudulent activity.

Managers are required to conduct and monitor fraud risk assessments and implement appropriate controls. They are required to monitor their fraud risk strategies and action plans as workplaces change.

7.8 Fraud Detection
The department has adopted fraud detection procedures to deal with fraud as soon as possible after it has occurred. Easily accessible reporting mechanisms are available on the department’s internet and intranet to ensure, staff, clients and the public can report allegations of fraud against recipients of funding administered by this department, or allegations of unlawful conduct by staff of the department.

Other detection controls in place at the department include review, analyses, reconciliations and audits. The department undertakes targeted reviews of its peripients where there is a high level of risk or a perceived risk of fraud. Staff of the department, play an important role in detecting fraud because of their technical expertise and knowledge of work practices and procedures.

7.9 Fraud Response
The department investigates allegations of fraud against the department and/or its programs and services in accordance with the Commonwealth Fraud Control Framework (the Framework) and Australian Government Investigation Standards (AGIS). All allegations of fraud, whether internal or external, are assessed with the aim of proving or disproving the allegations. Investigators in the department are required to attain minimum competency qualifications prescribed in the Framework.

The department’s Fraud Control Section, through the Fraud Investigation Unit, delivers criminal investigation services to the department and provides feedback on outcomes to the relevant departmental programs and the Assurance and Audit Committee.

Serious and complex cases of fraud may be referred to the Australian Federal Police (AFP). Occasionally, matters may also be referred to any of the State and Territory Police Services. Matters investigated by the department may be referred to the Commonwealth Director of Public Prosecutions (CDPP) for consideration of prosecution action.

The department has a policy where it will actively pursue the recovery of any money or property lost through fraud, provided there is a strong prospect of a net benefit to the department from such action.

7.10 Fraud Monitoring, Evaluation and Reporting
This Fraud and Corruption Control Plan (FCCP) is subject to regular monitoring and review, to ensure internal and external fraud controls and strategies are implemented and effectively achieving intended outcomes.

Quarterly reports are provided to the Executive and Assurance and Audit Committee. The department must certify in the Annual Report that the department has prepared fraud risk assessments and has a contemporary Fraud and Corruption Control Plan in place. Additionally, the department responds to the annual Australian Institute of Criminology survey on instances of fraud.
7.11 Fraud and Corruption Strategy and Action Plan

The Fraud and Corruption Strategy and Action Plan provides for a significant program of fraud control reform in the department. Driving significant and sustainable cultural change, whilst strengthening integrity governance arrangements and transitioning our reactive fraud program to a preventative proactive fraud control and anti-corruption framework.

8. Fraud Control Policy and Principles

The department considers fraud against the Commonwealth as a serious matter. In this regard, the department:

- maintains a ‘zero tolerance’ attitude towards fraud and requires that any case of suspected fraud is reported immediately and, dealt with appropriately
- creates and maintains an ethical culture in the workplace which supports vigilance, diligence, loyalty and the courage to report fraud-related concerns
- provides mechanisms for reporting allegations of internal and external fraud, and
- adopts a risk management approach to determine appropriated fraud control strategies.

To support these principles, the department will:

- ensure a fraud control plan is published and maintained in accordance with the Commonwealth Fraud Control Framework (the Framework)
- publish fraud control policies containing clearly documented fraud control procedures
- conduct divisional fraud risk assessments at a minimum of every two years or when there are significant changes to the structure and/or function of the department
- increase awareness of the risks of fraud by providing fraud awareness training to new staff at induction and through on-line training
- provide periodic fraud awareness training to ongoing staff and contractors which is designed to target a variety of audiences including high risk areas
- require professional and ethical practice by staff, consultants/contractors and those who do business with the department
- provide easily accessible mechanisms for reporting allegations of internal and external fraud
- maintain a FCO to provide oversight of all fraud control measures established by the department
- use all lawful avenues to recover money or property lost through fraudulent activity
- investigate allegations of fraud against the department, whether internal or external, in accordance with AGIS
- where appropriate, prepare briefs of evidence and refer matters to the CDPP for consideration of prosecution action, and
- ensure all aspects of fraud control are continuously monitored, reported and reviewed.

9. Fraud Roles, Responsibilities and Accountabilities

In order to ensure the department’s fraud control strategies are properly implemented, responsibilities for fraud control are clearly defined. This includes the designation of a FCO along with specific responsibilities for employees, management and the Secretary.

9.1 Overall Responsibility for Fraud Control

In accordance with Section 10 of the PGPA Rule, the Secretary has overall responsibility for fraud control within the department and developing and implementing the Fraud and Corruption Control Plan.

All staff have a vital role in the prevention and detection of fraud as part of their normal responsibilities. All staff are responsible for identifying potential fraud and considering fraud control at all stages of a programme’s lifecycle.

9.2 Authorised Official – Fraud Control Officer (FCO)

The Secretary authorised the department’s FCO to coordinate the development and implementation of a Fraud and Corruption Control Plan (FCCP) for the department, in accordance with Section 10 of the PGPA Rule and AAI 1.2.
10. How to Report Fraud and Other Suspicious Activity

The department accepts reports of suspected fraud from internal and external parties. The department ensures the confidentiality of the information received from any party wishing to report a suspected case of fraud.

All staff are expected to play a part in the identification and reporting of instances or events of suspected fraud. Allegations or suspicions of fraudulent activity must be reported to the Fraud Control Officer (FCO). A report can be made in person, in writing, by email, telephone or online.

10.1 Fraud Reports from Internal Parties

Details of the department’s fraud hotline, and other means by which fraud can be reported is part of both online and face-to-face fraud awareness training provided to staff. It is also contained within both the intranet and internet pages to ensure that people external to the department can be appropriately report allegations of fraud or corruption.

A report can be made in person, in writing, by email, telephone or through the department’s secure online reporting platform, Whispli.

- **Phone**: the department’s Fraud Control Hotline is: 02 6213 6376
- **Online**: Whispli Fraudsec https://app.whispli.com/fraudcontrolportal
- **Email**: fraudcontrolofficer@industry.gov.au
- **Post**: Fraud Control Officer
  Department of Industry, Innovation and Science
  GPO Box 2013
  Canberra ACT 2601

10.2 Fraud Reports from External Parties

Allegations of fraud by recipients of funding administered by the department, or allegations of unlawful conduct by staff of this department (or its contractors) can also be made via the same methods for internal staff (refer to Section 10.1 Fraud Reports from Internal Parties).

Further information is also available on the department’s internet site at www.industry.gov.au

10.3 Fraud Advice

The FCO has the authority to provide confidential and independent advice to staff and management in relation to concerns around suspected fraud.

Staff and managers are to be guided by the advice of the FCO and are to refrain from any action which might contaminate potential evidence or jeopardise the success of an investigation.

The FCO will also be responsible for maintaining an appropriate recording, reporting and analysis system to ensure that all instances of suspected fraud are satisfactorily resolved.

- the information provided to the FCO should include:
  - details and dates of the suspected offence
  - details of any staff involved (name and location)
  - the value of the alleged fraudulent or improper conduct
  - details of any clients or outside parties involved (name, description and address), and
  - potential sources of additional information about the matter in question, such as people and files.

All reported incidents are recorded and documented in accordance with Commonwealth requirements.

Fraud reporting information is also available on the department’s intranet and internet.

---

**More about Whispli...**

The advantage of using this online reporting platform is that while a two way conversation via email can be established, a user can choose to remain totally anonymous as Whispli scrubs all identifying features from where the report is made.

Whispli can also be accessed by downloading the following QR code
10.4 Reporting other usual and suspicious activity

If staff notice or suspect any unusual activity, they should contact Security Services:

Phone: 02 6102 8179
Email: securityservicesteam@industry.gov.au
Lodge a request: 02 6213 7007 or 1800 000 384

Insider Threats and Contact Reporting (see section 5.4) can also be reported to Security Services.

Cyber and Digital Fraud (see Section 5.5) can be reported to the ICT security team by email at itsa@industry.gov.au.

10.5 What to Expect When You Report Fraud

The department takes all allegations of fraud seriously. Information is assessed and, where appropriate, will be investigated. Should informants choose to provide personal details when making an allegation, an investigator may be in contact to obtain further information. They should also be aware they may be asked to provide a witness statement and give evidence in court.

Due to privacy restrictions and the integrity of the investigative process, you may not be provided with information regarding the progress of the investigation. Similarly, unless you agree to provide a statement and attend court, the fact that you have made the complaint will not be divulged by investigators.

Any reports to Personnel Security will be investigated in consultation with the Fraud team to determine the direction of the investigation. Should a full investigation be warranted, witness statements will be collected and used as required.

Occasionally staff may report suspicious behaviour to ICT Security directly in regards to witnessing a potentially fraudulent act. The ICT Security team records this as part of their investigation management process, and then forwards the report immediately to the Fraud Investigation team for further assessment. ICT Security ensures that all reports of fraud (suspected or confirmed) are treated sensitively, and unless there is a legitimate requirement to share an identity (such as when presenting in court), the team endeavour to maintain anonymity on behalf of the reporter. When providing quarterly reports to the Executive in regards to all investigations undertaken and assisted with, all staff names and titles are redacted prior to reporting.

10.6 Protection of Employees Reporting Suspected Fraud

The department will, in accordance with relevant policies and procedures, protect any person who has made an allegation against another member of staff or against an external party whether the allegation has been made with full disclosure of the informant’s identity or anonymously.

10.7 Public Interest Disclosure

The Public Interest Disclosure (PID) scheme, established by the Public Interest Disclosure Act 2013, came into effect on 15 January 2014. The PID scheme replaces the former whistleblowing provisions within the Public Service Act 1999 and provides a new legislative framework for the disclosure and investigation of serious wrongdoing within the Commonwealth public sector.

The PID scheme does not replace the other avenues available for the reporting of suspected wrongdoing within the department (such as reporting to a Fraud Control Officer or action under the department’s Code of Conduct procedures) but instead the PID scheme supplements these.

All departmental staff and contractors are encouraged to report suspected wrongdoing within the workplace utilising our existing mechanisms and PID scheme where applicable. The department is committed to ensuring that suspected wrongdoing covered by the PID scheme, such as corruption, breaches of law and maladministration, is appropriately investigated and addressed. The department is also committed to ensuring that those individuals who make disclosures under the PID scheme are supported and protected from reprisals.

The department has established a PID Procedure which outlines the way in which the PID scheme will operate within the department. The PID Procedure is available on on iCentral and the department’s internet site, www.industry.gov.au.

10.8 Anonymity

The department accepts anonymous reports of suspected fraud. Informants are not required to provide contact details if they do not wish to do so.

10.9 Privacy

Personal information is protected in accordance with the Privacy Act 1988. Any personal information collected will only be used for the purposes connected to the investigation of the allegation.
11. Fraud Investigations

In accordance with the Commonwealth Fraud Control Framework, the department conducts its own investigations into suspected fraud against its programmes and services.

**Internal Fraud** is fraud committed by staff or contractors of the department against programme or non-programme areas.

**External Fraud** is fraud committed by persons external to the department including contractors, providers of goods and services, and recipients of Commonwealth benefits and funding.

All allegations of fraud on the department, whether internal or external, are assessed, and where appropriate, investigated with the aim of proving or disproving the allegations to the criminal standard of proof.

The department’s Fraud Investigation Unit (FIU) delivers criminal investigation services to the department and then provides feedback of the outcomes to the relevant departmental programs and the Assurance and Audit Committee. Where an investigation obtains sufficient evidence to meet the criminal standard of proof, the matter will be referred to the CDPP. The FIU also seeks to identify weaknesses in risk controls or programme design issues which increase the exposure to risk.

The department’s People and Planning Branch is responsible for dealing with alleged breaches of the APS Code of Conduct. The FIU and People and Planning Branch liaise where there is both alleged criminal and code of conduct breaches. Fraud investigations require proof ‘beyond reasonable doubt’, whereas breaches of the APS Code of Conduct are based on a civil standard of proof.

The department works closely with other Australian Government agencies responsible for fraud prevention and response to allegations of fraud.

11.1 The Role of the Australian Federal Police (AFP)

The AFP is the Commonwealth’s primary law enforcement agency and protects Commonwealth and national interests from crime in Australia and overseas. The AFP is Australia’s international law enforcement and policing representative, and a chief source of advice to the Australian Government on law enforcement issues. The AFP is the lead agency in the investigation of serious or complex fraud against Australian Government programmes and systems. The department’s resources, information and expertise are shared with the AFP to assist in investigations where considered by the AFP. The FCO is responsible for identifying and referring matters to the AFP for its consideration in accordance with AFP protocols.

11.2 The role of the Commonwealth Director of Public Prosecutions (CDPP)

The CDPP is an independent prosecution service established by the Parliament of Australia to prosecute criminal offences against the Commonwealth. The CDPP determines whether or not to commence prosecution action in accordance with the Prosecution Policy of the Commonwealth. The CDPP is also available to provide advice on questions of evidence and/or other legal issues that arise during an investigation.

Liaison between the department and the relevant offices of the CDPP is conducted in accordance with the principles identified in the Prosecution Policy of the Commonwealth. Liaison with the CDPP is encouraged as it is an effective way for the department to ensure that a proposed course of action, in relation to a specific investigation, is resource effective and in the public interest to pursue.

12. Risk Management

In accordance with the Fraud Guidance contained in the Framework, the department must:

- undertake a divisional fraud risk assessment and enterprise fraud risk profile at least every two years
- develop its fraud risk assessments and FCCP using a methodology consistent with the relevant recognised standards
- reassess fraud risks with any change in organisation structure, or any major new or changed policies
- review and refine its fraud risk strategies on an on-going basis in light of its experience with continuing or emerging fraud vulnerabilities
- consider the outcomes of the fraud risk assessment in the development of the annual audit work programme, and
- ensure that employees engaged in agency fraud risk assessments acquire or possess a Certificate IV in Government (Fraud Control) or equivalent qualifications at a minimum.

12.1 Fraud Risk Assessment Process

The department conducts a fraud risk assessment program that incorporates all divisions.

Fraud Risk Assessments are conducted ‘face-to-face’ with each division. This enables the division to raise any concerns directly with the fraud control team to ensure clarity and accuracy in compiling the assessment.
To maximise the effectiveness of the fraud risk assessment process, the assessments will:

- be comprehensive, covering as far as possible, all potential fraud risks in all divisions at all locations
- comply with relevant Commonwealth Standards
- separately considers inherent risk and internal control
- identify potential treatments to mitigate any unacceptable risks, and
- achieve an overall ranking of identified fraud risks and provide fraud minimisation strategies, where required.

The department's divisions and senior management are responsible for ensuring that the strategies and/or actions plans developed during the course of a fraud risk assessment process are continually reviewed, actioned and updated where necessary.

The department's enterprise fraud risk profile provides an overall view of the department's fraud risk and is made up the ratings from each Divisional Fraud Risk Assessment. The rating is generally based on the highest level rated by all divisions.

### 12.2 Risk Management Framework

The department’s Risk Management Framework sets out a systematic approach to guide how risk management is embedded across the department for all business operations and staff at all levels. Specifically:

- what is risk management
- the value of risk management
- how risk management is embedded in the organisation
- the risk culture that the department aspires to
- define and convey the departments risk appetite
- outline the department’s approach to embedding risk management
- tools and resources to support risk management
- establish the roles and responsibilities for managing risks
- building risk capability and continuous improvement.

The framework is designed in accordance with:

- international risk management standard – principles and guidelines (ISO 31000:2009)
- the Public Governance, Performance and Accountability Act 2013
- the Commonwealth Risk Management Policy.
13. Fraud Prevention Strategies

Central to the department’s fraud prevention strategy is the identification of current and emerging fraud risks through an ongoing fraud risk assessment programme.

The department has implemented a number of prevention strategies which are outlined below.

13.1 Fraud Awareness Training

The department provides formal fraud awareness training and ensures that all updates and changes to fraud-related policies, procedures, codes of conduct etc., are circulated to staff and consultants/contractors in a timely manner.

The department has further developed its fraud awareness training programme with the implementation of an online training package and the delivery of face-to-face training targeted to the specific needs of line areas. In addition, training attendance records are maintained and feedback surveys are used to establish the effectiveness of training sessions.

13.2 Employment Screening

The department has an ‘Entry Level Access Assessment’ process to ascertain a person’s suitability for employment, against a list of defined pre-requisites.

As part of the recruitment process, Protective Security will verify the prospective new employee’s identity and eligibility (citizenship). Managers and Selection Committees through the interview process are responsible to verify the prospective employees’ suitability for the position.

As the recruitment and selection process for contractors is not required to meet the same standards as the engagement of an on-going and non-ongoing employee, a separate Personnel Security Policy has been developed for the engagement of non-APS employees. Where necessary, security clearances are undertaken for the department by the Australian Government Security Vetting Agency based in the Department of Defence.

13.3 Leave Policies

The department’s Leave Policy details the policy principles and leave conditions applicable to all staff. Each year, managers will be advised of employees with more than 30 days accumulated recreation leave credits at 31 March. Employees will be required to develop a plan with their manager to have their recreation leave credits at no more than 40 days at the following 30 September.

Employees who still have in excess of 40 days recreation leave at 30 September each year may be directed, in writing, to take leave.

13.4 Declaration of Interest and Conflict of Interest Policy

The department ensures that its employees and where required, departmental boards and committees, understand the detrimental impact to the department of conflicts of interest and insider trading.

The Conflict of Interest reporting period is between 1 August and 30 September. Each year, employees and contractors are required to view the Awareness Tutorial and make a disclosure if this is relevant. Other situations where employees should watch the tutorial include:

- annually
- within four weeks of commencement
- within four weeks of changing divisions
- where there have been significant changes to your personal or work circumstances
- all AusIndustry employees – if a conflict of interest arises in relation to work being undertaken
- all SES must complete the Conflict of Interest disclosure form.
- employees and contractors who do not have access to ESS Aurion are required to complete an Employee Declaration Statement located on iCentral.

13.5 ICT Security

The department has implemented an ICT Security Policy to ensure employees are aware of the security environment and their individual responsibilities for security. The department provides its employees with training in ICT security procedures and the correct use of ICT systems. Managers are responsible for requiring that their staff attend ICT security awareness training sessions.

14. Fraud Detection Strategies

It is incumbent on line management to be alert to the potential for fraud and to take active steps to detect any fraud that occurs.

The FCO will work with line management and internal audit in applying the department’s findings from fraud risk assessments to formulate effective fraud detection systems.

The department has implemented a number of detection strategies which are outlined below.

14.1 Fraud Reporting Mechanisms

Internal and external fraud reporting mechanisms are available on the department’s intranet and internet. A reporting hotline has been established and information is available to assist parties to understand their rights and obligations. The reporting mechanisms ensure the confidentiality of the information received from anyone wishing to report a suspected case of fraud.
14.2 Internal Audit

Internal Audit is an independent function within the department that reports directly to the Assurance and Audit Committee. They conduct better practice assurance activities, audits and assurance advisory services which assist in the development of efficient and effective systems of internal control, risk management and corporate governance.

The results of the most recent fraud risk assessment is considered when developing the Annual Audit and Assurance Plan. This is also developed with a view to the department’s stated risk appetite for fraud and corruption to ensure that areas with the highest areas of risk are considered. Internal Audit is also located within the Legal, Audit and Assurance Branch which assists with collaborating on emerging fraud risks and issues identified as part of audit activities. Further, fraud risks are considered within each audit where relevant to determine whether controls satisfactorily address these risks.

14.3 Security

The Australian Government Protective Security Policy Framework (PSPF) ensures a consistent application of security measures across all areas of government. Many of these security risks are applicable to the fraud and control environment.

The department’s key security objectives include:
• protecting departmental information, assets and infrastructure from unauthorised access, sabotage, wilful damage, theft and disruptions.
• preventing unauthorised disclosure of classified information, whether deliberate or accidental.

The Fraud Control Section and department’s security team work closely on security risks of mutual concern.

14.4 Compliance Reviews

Divisions are responsible for implementing compliance mechanisms and monitoring compliance within their programme, policy and business areas.

14.5 ICT Compliance

The department may monitor its employees to ensure that they comply with all ICT security requirements. The security of ICT systems may be reviewed regularly by the department’s ICT Security Advisor.

A formal process is used when dealing with incidents affecting ICT security. Where a security breach has been committed by an employee or some other person concerning the department’s ICT systems, where it is considered that a criminal offence may have been committed, the violation shall be reported to the FCO. If required, the FCO will recommend further action. If the violation relates to a potential Code of Conduct issue, the department’s People and Planning Branch will be informed and decide on appropriate action.

Compliance with the department’s security policies and procedures coupled with the prompt reporting of security breaches, incidents and inappropriate contacts, will aid in safeguarding against identified and potential fraud events and security threats.

15. Fraud Response Strategies

In compliance with the Framework, the department conducts investigations into suspected fraud against its programmes and services.

The department adopts AGIS as a best practice model for the investigation of all offences under Commonwealth legislation.

The department has implemented a number of response strategies which are outlined below.

15.1 Investigation Resources

To ensure that there is reasonable assurance that investigations are performed and reported properly, the department has appointed a FCO to ensure fraud control is conducted by experienced personnel who are sufficiently independent of the area or the matter under investigation.

All investigators hold mandatory qualifications as outlined in the Framework. The AGIS provides minimum case handling standards for investigations. Copies of the AGIS are available from the AFP, who undertakes this function on behalf of the Heads of Commonwealth Operational Law Enforcement Agencies (HOCOLEA).

15.2 External Investigation Resources

Where the initial investigation discloses a complex situation beyond the department’s investigative capability, external expertise should be sought to carry out the investigation. The decision to obtain such external expertise will be at the discretion of the FCO. The department has a panel of investigation providers that can be utilised as appropriate.
15.3  **AFP Referrals**

If a preliminary assessment indicates a matter is of sufficient seriousness that should be referred to the AFP, the following arrangements will apply:

- the possibility of action being taken under the *Proceeds of Crime Act 1987*
- conflicts of interest and/or politically sensitive matters
- sufficient information and/or evidence should be available to form the basis of a reasonable cause to suspect an offence may have been committed or attempted
- the matter should be of a fraudulent nature within the terms of the definition of fraud
- the suspected fraud or attempted fraud is considered serious and/or complex. The framework specifies that the existence of any of the following factors is an indication that a matter is serious or complex:
  - significant or potentially significant monetary or property loss to the Commonwealth
  - damage to the security, standing or integrity of the Commonwealth or a Commonwealth agency
  - harm to the economy, resources, assets, environment or well-being of Australia
  - a serious breach of trust by a Commonwealth employee or contractor of a Commonwealth agency
  - the use of sophisticated techniques or technology to avoid detection, that require 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 employee or contractor to a Commonwealth agency
  - known or suspected criminal activity against more than one Commonwealth agency
  - activities which could affect wider aspects of Commonwealth law enforcement (e.g. illegal immigration, money laundering).

The FCO is responsible for authorising referrals and subsequent liaison with the AFP and/or any of the state and territory police services, in relation to the department’s fraud investigations. The liaison requirement is on a case-by-case basis but some of the reasons for liaison are as follows:

- initial discussions as to the prospect of a referral of an investigation
- request for investigation assistance, such as a search warrant
- advice as to current law or procedures
- final referral of an investigation, and
- resource assistance to the AFP in their investigations.

15.4  **Disciplinary Procedures**

Where it is appropriate that the matter not be reported to the police, the department may pursue a range of remedies including dismissal, demotion or reprimand in accordance with the *Public Service Act 1998* and the APS Code of Conduct.

15.5  **Policy for Civil Proceedings to Recover the Proceeds of Fraud**

The department has adopted a policy wherein it will actively pursue the recovery of any money or property lost through fraud, provided there is a strong prospect of a net benefit to the department from such action.

16.  **Fraud Monitoring Reporting and Evaluation Strategies**

The department has developed and implemented appropriate information management systems and processes in accordance with the Framework and AGIS.

The FCCP is subject to regular monitoring and review, to ensure fraud controls are implemented effectively achieving intended outcomes. Significant change within the department may trigger an update of the FCCP to ensure it contains accurate and up-to-date information.

The Legal, Audit and Assurance Branch is responsible for the review, collection and collation of the controls that are in place (or that are proposed) to mitigate identified high level fraud risk. A formal review of these controls can be undertaken on a needs basis or as part of the routine fraud risk assessment activities.

The department has implemented a number of monitoring, reporting and evaluation strategies which are outlined below.
16.1 Fraud Control Reporting Requirements

<table>
<thead>
<tr>
<th>REPORTING TO:</th>
<th>REFERENCE/REQUIREMENT</th>
<th>REQUIREMENT</th>
<th>TIMEFRAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Board and Assurance and Audit Committee</td>
<td>Section 17AG PGPA Rule</td>
<td>The department must certify in each Annual Report that the department has prepared fraud risk assessments and a FCCP; and has in place appropriate fraud prevention, detection, investigation, reporting and data collection processes.</td>
<td>Annually</td>
</tr>
<tr>
<td>Annual Report</td>
<td>Section 17AG PGPA Rule</td>
<td>The department must report annually to the Minister, in a format to be determined by the department, on fraud risk control measures and outcomes.</td>
<td>Annually</td>
</tr>
<tr>
<td>Minister</td>
<td>Part II of Fraud Guidance</td>
<td>The department must report significant fraud incidents to the Minister as soon as practical.</td>
<td>Event specific</td>
</tr>
<tr>
<td>Minister</td>
<td>S 19 of PGPA Act</td>
<td>The department must report significant fraud incidents to the Minister as soon as practical.</td>
<td>Event specific</td>
</tr>
<tr>
<td>Australian Institute of Criminology (AIC)</td>
<td>Part II of Fraud Guidance</td>
<td>The department must collect specific fraud control information and provide it to the AIC by 30 September each year.</td>
<td>Annually</td>
</tr>
<tr>
<td>Australian Federal Police (AFP)</td>
<td>Part 10 of Fraud Guidance</td>
<td>The Australian Federal Police may conduct Quality Assurance Reviews (QARs) of the department’s investigations, in accordance with the AGIS. The outcomes of any QAR will be provided to the Attorney Generals Department.</td>
<td>Event specific and/or on formal request</td>
</tr>
<tr>
<td>Australian National Audit Office (ANAO)</td>
<td>The Framework Part II.3</td>
<td>The department’s compliance with the Fraud Rule may be the subject of audit by the ANAO.</td>
<td>ANAO initiated.</td>
</tr>
</tbody>
</table>

The department has developed and implemented information management processes to manage fraud control activities in accordance with the Framework and AGIS. Further information can be obtained from the FCO.

16.2 Insurance

The department maintains an insurance policy with Comover (DP 1.5) that insures the organisation against the risk of a financial (insurable) loss. Insurance for externally instigated fraud will all be maintained as appropriate including insurance against the theft of departmental property.

Insurance is reviewed annually in accordance with Commonwealth requirements.

For more information refer to Attachment A – Frequently Asked Questions.
## Frequently Asked Questions

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who</strong></td>
<td>The Fraud and Corruption Control Plan is owned by the Secretary. The Secretary has overall accountability and responsibility for fraud control, ensuring there are sound fraud control frameworks and governance mechanisms in place that comply with the Framework to effectively support fraud control activities. The department’s Assurance and Audit Committee provides independent assurance and advice to the Secretary on the operation of key controls and the Fraud Control Plan to the extent that it is within the charter. The Fraud and Corruption Control Plan is managed by the FCO and referenced by all levels of management. The FCO collects, collates and reviews the fraud risk management strategies and controls implemented by the department. A key responsibility of the FCO is ensuring the department meets and or exceeds the Framework.</td>
</tr>
<tr>
<td>Who reviews and evaluates the fraud and corruption control plan?</td>
<td>The department's Assurance and Audit Committee provides independent assurance and advice to the Secretary on the operation of key controls and the Fraud Control Plan to the extent that it is within the charter. The Fraud and Corruption Control Plan is managed by the FCO and referenced by all levels of management. The FCO collects, collates and reviews the fraud risk management strategies and controls implemented by the department. A key responsibility of the FCO is ensuring the department meets and or exceeds the Framework.</td>
</tr>
<tr>
<td><strong>Who has to undertake fraud awareness training?</strong></td>
<td>Fraud awareness training is encouraged by the Secretary. All staff are encouraged to attend fraud awareness training and/or information sessions. The FCO designs and develops an ongoing fraud awareness training programme to raise awareness of fraud and fraud risks amongst all staff and contractors. Specialised training is available to high risk areas. Fraud awareness training is conducted alongside other related training such as the APS Values and Code of Conduct, the ethical culture of the department.</td>
</tr>
<tr>
<td>Who has to undertake fraud awareness training?</td>
<td>Fraud awareness training is encouraged by the Secretary. All staff are encouraged to attend fraud awareness training and/or information sessions. The FCO designs and develops an ongoing fraud awareness training programme to raise awareness of fraud and fraud risks amongst all staff and contractors. Specialised training is available to high risk areas.</td>
</tr>
<tr>
<td><strong>Who analyses the fraud risks in the organisation?</strong></td>
<td>The Corporate Division is responsible for implementing and managing the department’s Risk Management Framework and relevant support functions on a day-to-day basis. Further information relating to Risk Management is available on the intranet. The FCO works with business areas to ensure internal and external fraud related risks are identified and adequate controls are in place to mitigate the risk to an acceptable level. It is a requirement of the fraud guidance that all key controls in place to address high levels of fraud related risk are articulated in the Fraud and Corruption Control Plan. The Assurance and Audit Committee acts as an agent of and an advisory body to the Secretary in relation to risk management and fraud control. Further information relating to the Assurance and Audit Committee responsibilities is located in the department’s Audit Committee Charter, available on the intranet.</td>
</tr>
<tr>
<td>Who analyses the fraud risks in my work area?</td>
<td>Managers and General Managers must assist the Secretary by demonstrating a high level commitment to fraud control and management and ensure business processes are planned and implemented after due consideration to fraud risk exposure. Business areas responsible for managing a particular fraud risk should be identified and the timeframes for implementing remedial action should be clearly documented in the risk management plans.</td>
</tr>
<tr>
<td><strong>Who analyses the fraud risks in my work area?</strong></td>
<td>Managers and General Managers must assist the Secretary by demonstrating a high level commitment to fraud control and management and ensure business processes are planned and implemented after due consideration to fraud risk exposure. Business areas responsible for managing a particular fraud risk should be identified and the timeframes for implementing remedial action should be clearly documented in the risk management plans.</td>
</tr>
<tr>
<td>What are the drivers of fraud risk at the organisation/program level?</td>
<td>The demand for timelines and flexibility in service delivery can create challenges in maintaining the integrity of the department’s programs. The risk of fraud can come from inside the department or from external parties such as clients, consultants, service providers, corporate entities or members of the public. The risk of programs being susceptible to fraud should be considered during the development, implementation and or delivery of Departmental programs.</td>
</tr>
<tr>
<td>What are the drivers of fraud risk at the organisation/program level?</td>
<td>The demand for timelines and flexibility in service delivery can create challenges in maintaining the integrity of the department’s programs. The risk of fraud can come from inside the department or from external parties such as clients, consultants, service providers, corporate entities or members of the public. The risk of programs being susceptible to fraud should be considered during the development, implementation and or delivery of Departmental programs.</td>
</tr>
<tr>
<td><strong>What is my role in fraud control?</strong></td>
<td>The identification and reporting of fraud is the responsibility of all staff and contractors. All staff and contractors play a part in managing the department’s potential exposure to fraudulent activity in a number of ways. Firstly, by ensuring they themselves behave in an ethical way consistent with the APS Code of Conduct and values. Secondly, by being alert to behaviour in the workplace that they suspect may be fraudulent and be prepared to report it expediently to the relevant point of contact. Thirdly, by being alert to indicators of potential external fraud being perpetrated on the department and being prepared to report it expediently to the relevant point of contact.</td>
</tr>
<tr>
<td>What is my role in fraud control?</td>
<td>The identification and reporting of fraud is the responsibility of all staff and contractors. All staff and contractors play a part in managing the department’s potential exposure to fraudulent activity in a number of ways. Firstly, by ensuring they themselves behave in an ethical way consistent with the APS Code of Conduct and values. Secondly, by being alert to behaviour in the workplace that they suspect may be fraudulent and be prepared to report it expediently to the relevant point of contact. Thirdly, by being alert to indicators of potential external fraud being perpetrated on the department and being prepared to report it expediently to the relevant point of contact.</td>
</tr>
<tr>
<td>What is a proportionate response to fraud risks in my organisation/work area?</td>
<td>Under the Framework, the department is required to investigate minor and routine instances of fraud, irrespective of whether the outcome of the investigation results an administrative remedy or is referred for criminal prosecution consideration. Matters involving serious and complex fraud must be referred to the AFP.</td>
</tr>
<tr>
<td>What is a proportionate response to fraud risks in my organisation/work area?</td>
<td>Under the Framework, the department is required to investigate minor and routine instances of fraud, irrespective of whether the outcome of the investigation results an administrative remedy or is referred for criminal prosecution consideration. Matters involving serious and complex fraud must be referred to the AFP.</td>
</tr>
<tr>
<td>When</td>
<td>Where</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>When do I get involved in fraud prevention and detection strategies?</td>
<td>Where can I find my organisation's Fraud Policy?</td>
</tr>
<tr>
<td>Whenever programmes are developed, new opportunities to perpetrate fraud may arise from internal and external parties. The risk of fraud should be considered at each critical stage of the programme lifecycle including, policy development, programme design, procurement, deliver/implementation/management and closure. All staff, in conjunction with their compliance teams, have prime responsibility for identifying potential fraud. The FCO will liaise with business areas and provide fraud awareness training to assist in ensuring staff of their responsibilities in relation to fraud control.</td>
<td>The department's Fraud Policy Statement is provided in DP1.2. It is also provided in fraud awareness training.</td>
</tr>
<tr>
<td>When do we report fraud in the organisation?</td>
<td>Where is the guidance on how to report fraud in my organisation?</td>
</tr>
<tr>
<td>Staff, contractors and external parties are encouraged to report all suspicions of fraud. This could include reporting concerns involving other staff, contractors or service providers. Where the business area suspects fraud, they may initiate discussions with the FCO to assist them in determining whether the issues should be referred.</td>
<td>All allegations of fraud on the department, whether internal or external, are assessed, and where appropriate, investigated with the aim of proving or disproving the allegations. Referrals of fraud should be delivered to the FCO following guidance provided in AAP1.2. These allegations may in turn be referred to the AFP. The People and Planning Branch reviews alleged APS Code of Conduct breaches, and works with the FCO to review internal allegations of fraud.</td>
</tr>
<tr>
<td>When do we analyse potential fraud activity?</td>
<td>Where can I refer matters of serious and complex fraud?</td>
</tr>
<tr>
<td>The risk analysis of programmes being susceptible to internal and external fraud should be considered during the development, implementation and/or delivery of departmental programmes.</td>
<td>All allegations of fraud on the department, whether internal or external, are assessed, and where appropriate, investigated with the aim of proving or disproving the allegations.</td>
</tr>
<tr>
<td>How</td>
<td></td>
</tr>
<tr>
<td>How do I get assurance that fraud risks are addressed in programme design?</td>
<td>How do I know our fraud strategies are working in my organisation?</td>
</tr>
<tr>
<td>How do I know our fraud strategies are working in my organisation?</td>
<td>How does my organisation decide if a suspected fraud will be investigated?</td>
</tr>
<tr>
<td>How do I get assurance that fraud risks are addressed in programme design?</td>
<td>How does my organisation decide if a suspected fraud will be investigated?</td>
</tr>
</tbody>
</table>