



Australian Government



Services  
Australia

# Fraud and Corruption Control Plan 2025–2026

January 2025





## Acknowledgement of Country

Services Australia acknowledges the Traditional Custodians of the lands we live on. We pay our respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

---

## Contents

Foreword	3
Introduction	4
Definitions	6
Fraud and corruption landscape	8
Governance	11
Fraud and corruption control approach	14
Reporting fraud and corruption	16

# Foreword

Our agency holds an important position of trust in this country. It's our responsibility to deliver billions of dollars in government payments and services with integrity, while holding and protecting sensitive information for nearly all Australians. We take these responsibilities seriously.



The Services Australia Fraud and Corruption Control Plan (the plan) is a critical document to outlining how we combat fraud and corruption risks, and instil a pro-integrity culture across our agency.

Effective fraud and corruption control is critical to our ability to deliver simple, helpful, respectful, and transparent services. That's why it's so important that we stay ahead of, and address, evolving fraud and corruption threats and new and emerging technology. The plan lays out how we will continue adapting and maturing our approach to fraud and corruption control to ensure the integrity of our services.

At the heart of this plan is a collective responsibility to build a strong pro-integrity culture of fraud and corruption prevention across every team, to underpin organisational health critical to building staff and stakeholder trust in the agency. This includes increased accountability at the program management level and streamlined reporting aligned with corporate goals.

The plan works alongside our other protective policies to underpin our commitment to APS Reform priorities and embody integrity in everything we do. Specifically, this plan supports the agency's obligations under the *National Anti-corruption Commission Act 2022* and new provisions in the Fraud Rule under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

The plan also details how we'll work across government and with third parties to respond to scams and data breaches. We know that identity crime, scams and third-party data breaches result in significant and widespread harm to agency customers. We will collaborate with Commonwealth partners such as the National Anti-Scams Centre, run by the Australian Competition and Consumer Commission, and the National Office of Cyber Security to align our objectives and actions with whole-of-government efforts to address scams and third party data breaches.

While senior leaders have specific accountabilities to meet, every staff member plays a vital role in maintaining robust defences. As experts in their roles, staff are best positioned to identify and address vulnerabilities.

Through our shared efforts, and working alongside our Commonwealth counterparts, we can ensure that we remain the trusted and resilient agency our customers expect.

**Chris Birrer**  
Deputy Chief Executive Officer  
Payments and Integrity Group

# Introduction

Services Australia is the Australian Government's primary service delivery agency; trusted to deliver over \$219.5 billion<sup>1</sup> in payments and services and hold sensitive, personal information of most Australians.

We recognise this position of trust, and the importance of protecting the integrity of government outlays and information. The agency's operating expenses in 2022–23 were approximately \$5.5 billion<sup>1</sup>. It is our duty to ensure these funds are used for the purpose for which they are provided.

The agency is dedicated to protecting our customers<sup>2</sup> and stakeholders from the risk of fraud and corruption perpetrated by malicious actors and corrupt individuals. This is done by implementing robust ethical standards, comprehensive monitoring systems and providing continuous education and support to foster a transparent and accountable environment.

We take fraud and corruption, and related crimes, seriously and take a strong stance to prevent, detect and respond to identified fraud and corruption.

We will undertake activities outlined in this plan and the agency's Enterprise Fraud and Corruption Risk Management Plan (FCRMP), while at the same time having the flexibility to adapt to change.

This plan articulates how the agency controls fraud and corruption, and assist in meeting the CEO's legislative obligations, as the accountable authority, under Section 10 of the *Public Governance, Performance and Accountability Rule 2014* (PGPA Rule).

The plan also supports the agency's guiding principles (simple, helpful, respectful and transparent) and the Privacy Management Plan. It enables the agency to simplify processes while respecting and protecting personal information and reducing potential harm to the agency's programs, payments and customers.

<sup>1</sup> Services Australia Annual Report 2022–23.

<sup>2</sup> Agency definition of a customer – Individuals or parties interacting with Services Australia about past, present or future access to payments and services.



## Simple

- Pathways and processes that minimise steps
- Easy access to the services and support customers need
- 'Tell us once' principles applied to customers' personal details and information



## Helpful

- Informed staff who provide proactive, personalised services
- Help with information and what to do next
- Advice on options based on a customer's situation



## Respectful

- Supportive staff who listen to and understand customers' needs
- Servicing options that respect customers' time and situation
- A welcoming environment



## Transparent

- Help to understand the process and what to do next
- Information about how data is used
- Clarity about the reason for decisions

# Commonwealth Fraud and Corruption Control Framework 2024

The Commonwealth Fraud and Corruption Control Framework 2024 sets out and details the requirements for effective fraud and corruption control in all Commonwealth entities. The framework consists of 3 parts:

Section 10 of the PGPA Rule	Commonwealth Fraud and Corruption Policy	Resource Management Guide No. 201
The rule is a legislative instrument for all PGPA Act entities. It requires Commonwealth entities to take all reasonable measures to prevent, detect and respond to fraud and corruption).	This policy sets out mandatory procedural requirements that must be implemented for fraud and corruption control.	This provides further guidance on how to meet requirements.

## Fraud and Corruption Control System

The agency's Fraud and Corruption Control System outlines how our activities in this space meet the requirements of the Commonwealth's Fraud and Corruption Control Framework.

### Services Australia Accountable Authority Instructions

Section 1.1: Prescribes that all officials are responsible for actively managing risks and complying with the Commonwealth Risk Management Policy.

Section 1.3.1: Prescribes that staff comply with the Commonwealth Fraud Control Policy and must act in accordance with the agency's Fraud and Corruption Control Plan.

### Risk Management Policy and Framework

Articulates the direction and approach for managing risk in the agency. It incorporates the Risk Management Policy and arrangements for embedding risk management throughout the agency.

### Enterprise Fraud and Corruption Risk Management Plan

The agency's Enterprise FCRMP is a high-level risk assessment of our exposure to fraud and corruption, which provides a landscape view of all activities, functions and expenditure areas and our operating environment.

### Services Australia Fraud and Corruption Control Plan

The Services Australia Fraud and Corruption Control Plan articulates how we align and satisfy our obligations under the Commonwealth Fraud and Corruption Control Framework 2024.

### Associated legislation, agency policies and processes

We manage fraud and corruption with complementary and layered support with the following:

- Payment Assurance Strategy
- Protective Security Plan 2023–25
- Cyber Security Policies and Strategy
- Privacy Management Plan 2024–25
- Integrity Framework
- Operational FCRMPs
- Data Governance Framework
- Group and Program area risk management plans
- Employment Principles, the Code of Conduct and APS Values, as set out in the *Public Service Act 1999*.
- Portfolio Program and Project Assurance Framework

# Definitions

## Fraud

All fraud requires intent. Fraud can be committed internally by agency staff (including labour hire, contractors), or externally by customers, members of the public, third party organisations and service providers, or online thieves. It may also be committed through collusion between an employee and outside party. It can involve financial and non-financial incidents that impact on the agency's operations, delivery of services or undermine public confidence in Services Australia or the Commonwealth.

Offences of fraud against the Commonwealth may be prosecuted under several Commonwealth laws, including the *Criminal Code Act 1995* or the *Crimes Act 1914*.

### **Fraud is defined in the Commonwealth Fraud and Corruption Control Framework 2024 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** occurs when employees, labour hire or contractors within the agency:

- misuse staff entitlements (such as medical leave, travel or overtime)
- access or disclose information (such as customer or official information) without authority
- inappropriate use or theft of agency assets (such as IT equipment, mobile phones or fleet vehicles) for personal benefit
- use system access to create fraudulent payments or redirect payments
- manipulate procurement or recruitment processes
- use their inside knowledge to make false claims for payments as customers of the agency.

**External fraud** occurs when customers or other third parties:

- deliberately provide false or misleading information to make a claim for a payment or service
- assume, or attempt, to assume another person's identity to gain a benefit or advantage
- redirect another person's payment, where there is no legal basis for doing so
- provide false evidence for services or goods not provided
- access our information and systems without authority.

This includes systemic and organised criminal targeting of the agency with these actions.

## Corruption

Corruption may be criminal or non-criminal in nature and may affect any aspect of public administration. For example, an official being offered or accepting a bribe, or engaging in fraud against the entity.

**Corruption is defined in the Commonwealth Fraud and Corruption Control Framework 2024, and broadly consistent with the National Anti-Corruption Act 2022, as:**

Any conduct that does or could compromise the integrity, accountability or probity of public administration. This includes:

- any conduct of any person (whether or not a staff member of a Commonwealth agency) 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.
- 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 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.

## Non-compliance

Non-compliance is a broad term for any failure to comply with legal or administrative requirements. These requirements may be in the form of legislation, regulation, funding agreements, administrative rules, licensing conditions, or agency policies. One example is the requirement for all Australian Public Service (APS) employees to act in accordance with the APS Code of Conduct, which is set out in Section 13 of the *Public Service Act 1999*.

Non-compliance includes where parties try to comply but make mistakes (accidental non-compliance). There are non-compliance activities that can be considered fraud which are managed through actions such as compliance reviews and debt activities by the agency.

## Unethical behaviour

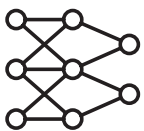
The APS Values and Code of Conduct describe a work ethic expected of the public service that includes honesty, diligence, avoidance of conflict of interest, and proper use of resources. Breaches of this code of conduct may constitute unethical behaviour and Services Australia has formal procedures for examining any potential breach.

# Fraud and corruption landscape

The Australian Institute of Criminology estimates that fraud against the Commonwealth was approximately \$160 million<sup>3</sup> in 2022–23. Fraud can be difficult to detect and, as such, the scale and cost to Australian society is often underestimated.

The Government's APS Integrity Action Plan is focused on driving a pro-integrity culture. The plan establishes systems to support effective fraud and corruption management, with clear accountability at all levels.

Corruption is experiencing a renewed scrutiny with the establishment in 2022 of the National Anti Corruption Commission (NACC), an independent federal Australian Government agency that was created under the *National Anti-Corruption Commission Act 2022*.



## Increased digitisation of Government services

As government services rapidly transition to digital platforms, fraud targeting online channels has surged. Our current efforts are being outpaced by technological advancements that expose vulnerabilities that need immediate attention.

Externally, there has been an increase in third party organisations and individuals experiencing data loss because of cyber breaches and scams. Such breaches expose personally identifiable information, including identity credentials, leaving individuals vulnerable to identity theft and increasing risk of misuse against agency programs, services, and platforms.



## Identity crime and organised crime

Identity crime generates large profits for offenders while causing major financial losses to the Australian Government, private industry, and individuals. A single identity crime investigation may involve multiple offenders and hundreds of victims.

Criminal actors and networks, both in Australia and overseas, and are systematically targeting government programs, particularly emergency payments and agency customers including our most vulnerable. These sophisticated criminal groups use adaptive techniques, pivoting between different payment streams and actively seeking to circumvent fraud controls. Their methods include rapid movement of fraudulent funds, for example multiple bank accounts, to dilute funds and avoid detection.

These activities pose a significant challenge to current investigative approaches and highlight the need for cross-government and cross-jurisdictional cooperation.



## Fraud is prevalent and increasingly complex

According to the Australian Institute of Criminology there are tens of thousands of instances of reported fraud and corruption against the Commonwealth each year. These acts are deliberately concealed by malicious actors and often overlooked by its victims.

The agency's large information holdings make it a target for insider threats, including through outside influences on our staff. The complexity of these threats require a coordinated response that includes law enforcement and other government agencies to safeguard the integrity of government payment and services.



## Building trust

Priority one of the APS Reform is 'An APS that embodies integrity in everything it does'. The government and community expect Commonwealth entities to act with integrity and fairness and be accountable and transparent in everything they do.

<sup>3</sup> Australian Institute of Criminology – Statistical Bulletin 44 Fraud against the Commonwealth 2022–23



## Fraud and corruption enterprise risks

Top Enterprise Risk	Enterprise fraud and corruption risks	Fraud and corruption sub-risk statements
<p><b>Performance</b></p>	<p><b>Agency payments and services</b></p> <p>Dishonest claims, theft or misdirection or payments and services administered by the agency.</p>	<p>Dishonest claims, theft, misdirection or misappropriation of social welfare payments and services administered by the agency.</p>
		<p>Dishonest claims, theft, misdirection or misappropriation of health payments and services administered by the agency.</p>
		<p>Dishonest claims, theft, misdirection or misappropriation of Child Support payments administered by the agency.</p>
		<p>Dishonest claims, theft, misdirection or misappropriation of aged care payments and services administered by the agency.</p>
		<p>Theft, misdirection or misappropriation of payments administered by the agency, including those on behalf of other government agencies under shared service arrangements.</p>
<p><b>Performance</b></p>	<p><b>Identity crime</b></p> <p>The agency accepts compromised, fabricated and/or manipulated identity information and/or credentials.</p>	<p>The agency fails to establish confidence in a customer's<sup>4</sup> identity when commencing delivery of a payment or service.</p>
		<p>The agency fails to establish a customer<sup>4</sup> is the person they say they are during each interaction, prior to accessing and/or disclosing personal information, payments or services.</p>
		<p>The agency fails to establish confidence in a Third Party Organisation<sup>5</sup> and/or a representative acting on behalf of a Third Party Organisation when the agency commences providing information, payments or services.</p>
		<p>The agency fails to establish an individual acting on behalf of a Third Party Organisation<sup>5</sup> is who they say they are during each interaction prior to accessing and/or disclosing information, payments or services.</p>

Top Enterprise Risk	Enterprise fraud and corruption risks	Fraud and corruption sub-risk statements
<b>Data</b>	<b>Information access or misuse</b>  Theft, modification, unauthorised access, use or disclosure of information and/or data.	Theft, modification, unauthorised access, use or disclosure of Services Australia's customer information by agency staff or contractors.
		Theft, modification, unauthorised access, use or disclosure of Services Australia's staff information and data, corporate information and corporate data by agency staff or contractors.
		Theft, modification, unauthorised access, use or disclosure by agency staff or contractors of other government agency and external organisation information and data held by Services Australia.
		Theft, modification, unauthorised access, use or disclosure of information and data by approved external parties.
		Theft, modification, unauthorised access, use or disclosure of information and data by unapproved external parties.
<b>Organisational Integrity</b>	<b>Agency funds and assets</b>  Theft, misdirection or misuse of agency funds and assets.	Fraudulent and inappropriate procurement activity, including allocation of program funding and contract or vendor management.
		Fraudulent or unethical recruitment practices.
		Fraudulent claims or use of employee entitlements, payroll fraud and misappropriation of agency funds.
		Theft, misuse or misappropriation of agency assets.

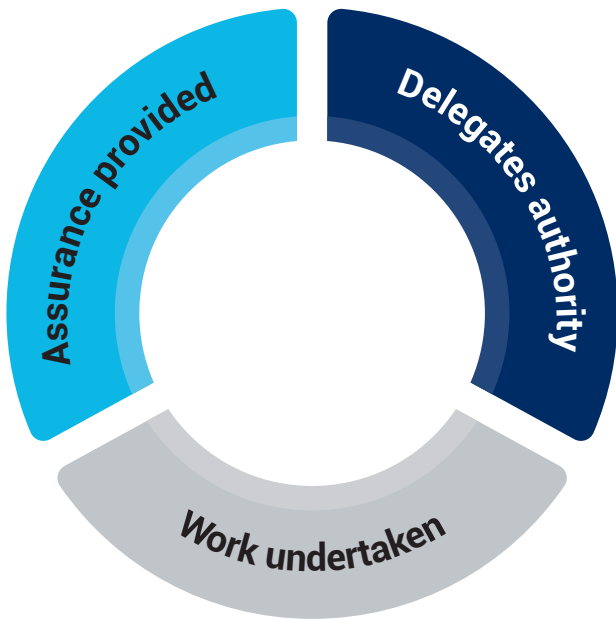
<sup>4</sup> Customer includes a customer or someone acting on behalf of the customer (i.e. Centrelink nominee, Medicare or Child Support authorised representative, Power of Attorney).

<sup>5</sup> Third Party Organisations include providers, delivery partners, advocates, other entities and government agencies that interact with the agency to receive payments or services, and access customer information.

# Governance

To embed strong governance and drive cultural change, the agency has a fraud and corruption accountability model aligned to our Risk Management Policy and Framework.

The governance model makes clear how all areas of the agency are responsible for their fraud and corruption risks.



### Accountability

The CEO is the Accountable Authority, they delegate authority and actions.

### Responsibility

Services Australia manages fraud and corruption risks through a THREE LINES MODEL.

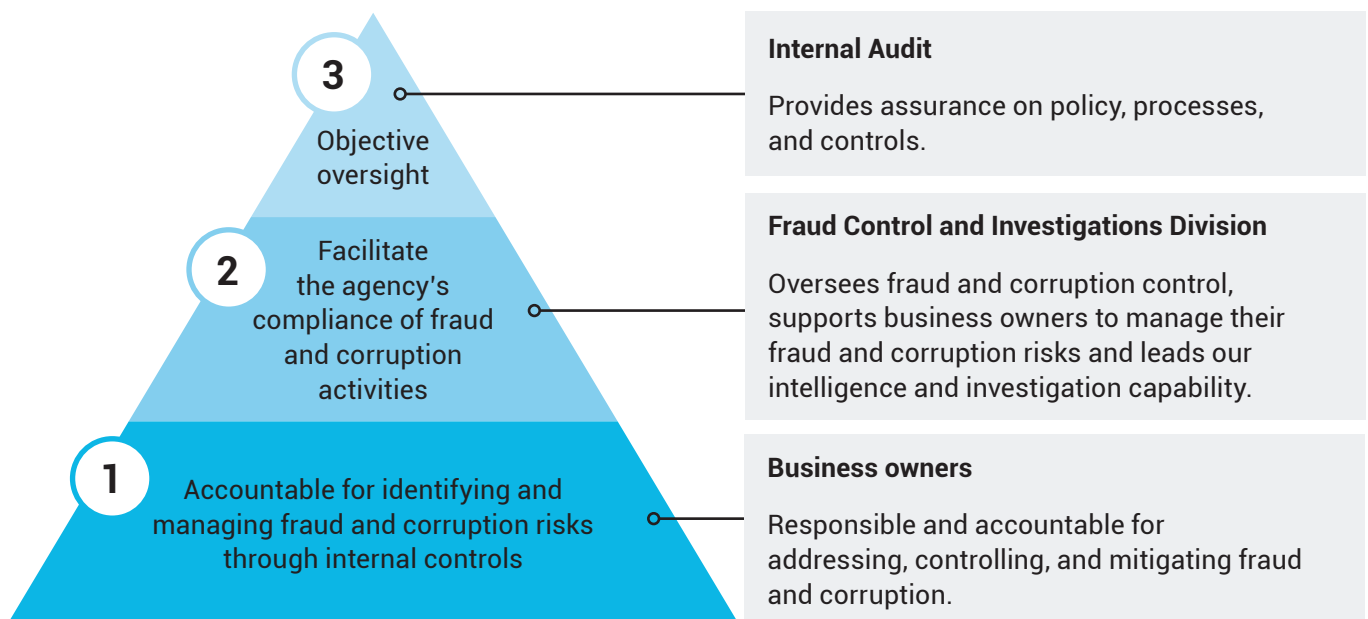
### Assurance

Assurance activities, reporting to governance committees and accountable authorities:

- Security Committee
- Executive Committee
- Audit and Risk Committee
- Deputy Chief Executive Officers.

## Three Lines Model

The Three Lines Model remains the foundation for how we manage fraud and corruption. The Model describes the roles and responsibilities of different officials in an effective fraud and corruption risk management approach.



### Internal Audit

Provides assurance on policy, processes, and controls.

### Fraud Control and Investigations Division

Oversees fraud and corruption control, supports business owners to manage their fraud and corruption risks and leads our intelligence and investigation capability.

### Business owners

Responsible and accountable for addressing, controlling, and mitigating fraud and corruption.

# Roles and responsibilities

Specific positions and committees within the agency have defined responsibilities for fraud and corruption control as outlined in the table below.

Owner	Responsibilities
<b>Chief Executive Officer (CEO)</b>	<p>Under section 10 of the Public Governance, Performance and Accountability Rule 2014, the CEO, as the Accountable Authority, must take all reasonable measures to prevent, detect and deal with fraud and corruption relating to the agency.</p> <p>The CEO, and officers with certain functions under the <i>Public Interest Disclosure Act 2013</i>, must refer serious or systemic corruption issues to the NACC.</p>
<b>Audit and Risk Committee</b>	<p>Provides the CEO with written advice on the appropriateness of the agency's fraud control arrangements to detect, capture and effectively respond to fraud and corruption risks consistent with the Commonwealth Fraud Control Framework. This process informs the Letter of Transmittal contained in the agency's Annual Report.</p>
<b>Executive Committee</b>	<p>The agency's most senior governance committee. This committee is responsible for supporting the CEO's accountability for the agency's strategic outcomes and performance, ensuring accountability and compliance with regulatory requirements.</p>
<b>Security Committee</b>	<p>Oversees the agency's security governance arrangements and ongoing management of information, personnel, cyber and physical security matters. This Committee provides an escalation point for risk relating to fraud and corruption, further escalating issues to the Executive Committee as required. They provide advice and recommendations on the implementation of this plan.</p>
<b>All staff</b>	<p>All staff are responsible for actively contributing to fraud and corruption risk management, identification, and escalation of risk, and must:</p> <ul style="list-style-type: none"> <li>• encourage and act to maintain a pro-integrity culture and environment that fosters personal responsibility, integrity and accountability</li> <li>• report any incident of suspected or potential fraud or corruption immediately</li> <li>• adhere to the APS Values and Code of Conduct</li> <li>• be aware of the agency's fraud and corruption control, risk management and protective security policy frameworks.</li> </ul>
<b>First Line: Responsible for their fraud and corruption risks within their group/division/branch</b>	
<b>Deputy Chief Executive Officer (DCEO)</b>	<p>Are accountable to the CEO for the day-to-day management of risks within their group and are jointly responsible for managing the agency's enterprise fraud and corruption risks.</p> <p>Individually DCEO's:</p> <ul style="list-style-type: none"> <li>• manage fraud and corruption risks in their group</li> <li>• are responsible for their group's contributions to the Enterprise FCRMP</li> <li>• drive a positive risk culture, by ensuring good risk management is embedded into their group's decision making processes</li> </ul>

Owner	Responsibilities
<b>First Line: Responsible for their fraud and corruption risks within their group/division/branch</b>	
<b>General Managers</b>	<p>Collectively responsible for encouraging and maintaining a pro-integrity culture and environment that foster personal responsibility, integrity and accountability.</p> <p>Individually, General Managers are:</p> <ul style="list-style-type: none"> <li>• accountable for identifying, managing, monitoring, reporting and escalating risks</li> <li>• responsible for implementing and monitoring treatments where the controls in place are ineffective and further mitigation activities are required.</li> </ul>
<b>National Managers</b>	<p>Collectively responsible for encouraging and maintaining a pro-integrity culture and environment that foster personal responsibility, integrity and accountability.</p> <p>Individually, National Managers are responsible as the first line for fraud and corruption risks in their programs and functions, including:</p> <ul style="list-style-type: none"> <li>• ensuring that all reasonable steps are taken to identify and manage fraud and corruptions risks, including implementing fraud and corruption controls in policy, processes, and systems, and that core systems are accredited</li> <li>• escalating fraud and corruption risks to their General Manager in accordance with the Risk Management Policy and Framework</li> <li>• implementing fraud and corruption risk treatments</li> <li>• addressing feedback from Fraud Control and Investigations Division on fraud and corruption risks, treatments and controls</li> <li>• reporting on operational fraud and corruption risks, treatments and controls.</li> </ul>
<b>Second Line: Facilitates the agency's compliance of fraud and corruption activities</b>	
<b>Fraud Control and Investigations Division</b>	<p>Manages fraud and corruption risks by:</p> <ul style="list-style-type: none"> <li>• delivering fraud and corruption intelligence and investigation capabilities</li> <li>• providing fraud and corruption risk management expertise to our agency and managing the agency's fraud and corruption risk and control plans and policies</li> <li>• providing feedback on fraud and corruption risks, treatment and control issues to program and function owners</li> <li>• identifying and assessing the agency's enterprise fraud and corruption risks and coordinating the agency's Enterprise FCRMP</li> <li>• supporting the development, maintenance and monitoring of processes to measure control effectiveness, identification of treatments in operational FCRMPs and informing relevant risk owners</li> <li>• undertaking Fraud and Corruption Control Assurance activities</li> <li>• maintaining our Enterprise Fraud and Corruption Risk Register and providing fraud and corruption risk reports to accountable senior executive</li> <li>• reporting fraud and corruption control activities to the Executive Committee, the Audit and Risk Committee and the Security Committee.</li> </ul>
<b>Third Line: Accountable for identifying and managing fraud and corruption risks through internal controls</b>	
<b>Audit Branch</b>	<p>Provides independent assurance that counter fraud and corruption activities and controls work as designed.</p>

# Fraud and corruption control approach

Services Australia's fraud and corruption control is built around the principles of prevention, detection and response, and includes a range of strategies designed to protect Services Australia and our staff, and customers.

## Prevention

Prevention is the most effective and cost-efficient means of countering fraud and corruption. The agency's prevention strategies include proactive measures designed to prevent fraud and corruption, and ensuring that fraud and corruption risks are considered in planning and conducting the agency's activities.

Early consideration of risk positions the agency to appropriately balance service delivery priorities such as streamlining processes and improving customer experience with safeguarding the integrity of our payments, services, resources and systems.

Agency prevention activities include:

- delivering targeted messaging and fraud and corruption awareness training to maintain a culture of integrity and ensure staff and third party providers understand the important role they have in fraud and corruption control
- assessing our enterprise fraud and corruption risks and managing and reporting actions to address these risks
- assessing and managing operational fraud and corruption risks
- proactively working to ensure that both internal and external fraud and corruption control is considered in the design and development of policies, programs, systems and processes
- providing expert advice, tools and guidance to support business owners with managing their fraud and corruption risks
- testing and verifying the effectiveness of fraud and corruption controls and co-design of fit-for-purpose treatments
- influencing policy settings internally and externally to achieve high levels of identity assurance and improving identity and authentication processes
- building, implementing and refining robust fraud and corruption risk detection profiles that allow us to focus our effort in areas of higher risk
- proactively using front end controls, including pre-payment fraud detection, third party data sets and system rules to help establish eligibility at the point of claim
- collaborating with government partners to prioritise high profile criminal targets that deliberately exploit government programs
- using a strategic network of national and internal partnerships in fraud and corruption management to understand emerging threats and implement best practice counter measures
- implementing robust recruitment and pre-engagement screening processes
- requiring staff to obtain and maintain security clearances where the role requires access to security classified information or systems, or where additional assurance of the suitability and integrity of personnel is required
- sharing intelligence and working across government, law enforcement and international jurisdictions
- providing advice and support to agency customers (including myGov users) about scams (including those purporting to represent the agency) and circumstances where their personal information has been stolen or lost
- completing ethical declarations in relevant procurement and processing activities.

## Detection

Despite the agency's best preventive strategies, not all fraud risks can be eliminated. The agency has effective detection processes including up-front and back-end detection activities. These include:

- making it easy for staff to report suspicious activity, and communicating strategic examples so that staff recognise the benefit of their actions
- utilising a comprehensive internal and external tip-off program to identify criminal activity
- creating, refining and maintaining strategies for detecting fraud and corruption threats
- assessing fraud and corruption reports and allegations to determine an appropriate response
- collaborating across government to identify fraud and corruption trends, and where possible using combined intelligence and data to detect common threats
- exploring the use of advanced data analytics including Machine Learning to detect potential fraud and corruption
- identifying scams that impersonate the agency, through public reporting and intelligence activities.



## Response

Any alleged fraudulent or corrupt behaviour that is reported to or detected by the agency will be handled appropriately, including:

- when an investigation is deemed appropriate, undertaking investigations in accordance with the Australian Government Investigations Standards (AGIS)
- pursuing disciplinary, administrative, civil, or criminal actions as appropriate
- pursuing recovery of fraudulently or criminally obtained benefits where appropriate
- undertaking joint-agency operations or referring to the Australian Federal Police (AFP) or other law enforcement bodies
- digital forensics capability, supporting whole of government efforts to combat criminal conduct through advanced digital forensic evidence extraction and analysis
- developing controls and treatments resulting from detection and response activities
- working with other stakeholders to respond quickly to scams, third party data breaches and mishandling of personal information that affect customers and their personal information, including adding security measures and remediating compromised customer records.

## Monitoring, evaluating, and reporting fraud and corruption

A key element to controlling fraud and corruption is ensuring that business areas and accountable executive make considered and evidence-based decisions. Fraud and corruption risk monitoring, evaluating, and reporting occurs at the enterprise, group and operational levels. This ensures that fraud and corruption risks are visible and accepted by risk owners and accountable executive.

We do this through:

- ✓ monitoring and evaluating controls, and adjusting specific controls to meet new or emerging circumstances
- ✓ assessment of fraud and corruption risk, through targeted activities
- ✓ continual improvement of fraud and corruption control processes and systems.

Regular fraud and corruption assurance reporting is an important part of effective governance and oversight. Internal and external assurance reporting occurs:

- quarterly to the Services Australia Security Committee
- biannually to the Services Australia Executive Committee and Audit and Risk Committee
- annually to the Australian Institute of Criminology.

We also report to the Commonwealth Ombudsman as required, in accordance with the requirements of the *Public Interest Disclosure Act 2013*.

# Reporting fraud and corruption

## Awareness and culture

All new Services Australia staff, including employees, contractors, consultants and secondees must complete fraud and corruption awareness training as part of the induction program and annually thereafter.

The agency also maintains regular communications targeted at promoting fraud and corruption awareness and a pro-integrity, ethical organisational culture that supports reporting.

## Fraud and corruption reporting mechanisms

Suspected fraud and corruption related to Services Australia can be reported in the following ways:

- submitting an anonymous tip-off via the Services Australia website [servicesaustralia.gov.au/individuals/contact-us/reporting-fraud](https://servicesaustralia.gov.au/individuals/contact-us/reporting-fraud)
- mail: Services Australia Reply Paid 7803 Canberra BC ACT 2610
- phone: Fraud tip-off line **131 524**

## Public Interest Disclosure (PID)

The *Public Interest Disclosure Act 2013* promotes 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. Services Australia will act on disclosures as appropriate and protect disclosers from any reprisals for making a disclosure.

As required by legislation, a person must be a current or former public official to report under the public interest disclosure scheme.

PIDs can be made orally or in writing:

- by an employee to their manager
- to an Authorised Officer
- to [PID@servicesaustralia.gov.au](mailto:PID@servicesaustralia.gov.au)

For more information, please refer to Services Australia's public interest disclosure procedures.

## National Anti-Corruption Commission (NACC)

The NACC operates independently of government. The NACC detects, investigates and reports on serious or systemic corruption in the Commonwealth public sector, and educates the public service, and the public, about corruption risks and prevention.

The NACC complements the agency's pro-integrity culture and provides an independent process to report suspected corruption. The *National Anti-Corruption Commission Act 2022* provides protection from reprisal for reporting suspected corruption.

The NACC investigates serious or systemic corruption and has the power to investigate parliamentarians – including Senators and Ministers and their staff, statutory officer holders, and employees and contractors of all government entities.

Reports about corruption can be made:

- online: [nacc.gov.au/reporting-and-investigating-corruption](https://nacc.gov.au/reporting-and-investigating-corruption)
- phone: **1300 489 844**
- Translating and Interpreting Service: **131 450**
- National Relay Service: **133 677** and ask for **1300 489 844**
- mail: National Anti-Corruption Commission GPO Box 605 Canberra ACT 2601

## Management of reports

Services Australia maintains appropriate systems to securely store, record, report and analyse allegations of fraud to ensure appropriate response and satisfactory resolution. All reported allegations are recorded and documented in accordance with Commonwealth requirements.

## Privacy

Services Australia ensures the confidentiality of the information received from anyone wishing to report a suspected case of fraud. All reports are managed in accordance with the *Privacy Act 1988* and the agency's Privacy Policies.

Where the report may be more appropriately considered by another agency or organisation, we may disclose this information (including your personal information) to that agency or organisation. This includes a federal, state/territory agency, department, or authority, and federal or state/territory Minister.





