Australian Government

Office of the Australian Information Commissioner

Fraud Control Plan and Risk Assessment

November 2023

13 November 2023

OAIC

Audience: Internal

Location: Intranet

Review date: November 2024

Version	Name	Changes	Date
1.0		Fraud Control Plan 2012-2014 approved by Australian Information Commissioner	1 January 2020
2.0		Fraud Control Plan 2014-2016 approved by Australian Information Commissioner	18 March 2014
2.2		Fraud Control Plan 2017-2019 approved by Australian Information Commissioner	29 August 2017
3.0		Fraud Control Plan 2021-2022 approved by Australian Information Commissioner	6 August 2021
4.0	Penny Ryder	Fraud Control Plan 2022-2023 approved by Australian Information Commissioner	April 2023
4.1	Penny Ryder	Additional updates to fraud risk control testing requirements following Fraud Maturity Assessment (internal audit) and to align contents with the Fraud Control and Corruption: Policy and Guidelines	November 2023

Contents

Introduction

The OAIC's policy position on fraud and fraud control is described in the *OAIC Fraud Control and Corruption: Policy and Guidelines* (the policy). Capitalised terms used in this document have the same meaning as in the policy unless otherwise indicated.

This Fraud Control Plan and Risk Assessment supports the policy and describes the controls being maintained by the OAIC to manage fraud risk. It is updated not less than every two years and contains two main sections:

- **General Fraud Control Strategies.** Broadly relevant foundational fraud control measures implemented to address systemic fraud concerns or as a reflection of good governance.
- **Fraud Risk Assessment.** The identification and analysis of specific fraud and corruption related risks and the controls in place to manage them in accordance with the OAIC Risk Management Policy and Framework.

Together, the policy and this document describe the OAIC's approach to:

- Preventing and detecting fraud and/or corrupt conduct; and
- responding to suspected fraud, incidents of fraud and/or corruption issues.

General fraud control strategies

Legislative, regulatory and policy compliance

The exercise of the OAIC's responsibilities and functions shall fully comply with the:

- *Australian Information Commissioner Act 2010*, *Privacy Act 1988* and the *Freedom of Information Act 1982* (the FOI Act).
- the PGPA Act), the PGPA Rule (including section 10 - the Fraud Rule), the Fraud Policy and the Fraud Guidance.
- *Public Service Act 1999* including the APS Values and Code of Conduct, and the *Public Service Regulations 2023*.
- *Crimes Act 1914*, *Criminal Code Act 1995*, *Proceeds of Crime Act 2002* and *Evidence Act 1995*.
- *Director of Public Prosecutions Act 1983* and *Auditor-General Act 1997*.
- the OAIC's Enterprise Agreement.
- Accountable Authority Instructions and other OAIC policies, in particular the OAIC *Risk Management Policy and Framework*.

The OAIC maintains a *Legislative Compliance Register* that fully details the legislation relevant to its work.

The OAIC regularly reviews and updates its Delegation Instruments, Accountable Authority Instructions, and other instruments.

Planning and business management

The OAIC's program, functions, and activities are articulated in the Corporate Plan and Branch plans and flow through to individual Performance Agreements. The Executive, Directors and staff will review and evaluate performance against plans on a regular basis.

Managing the risk of fraud and corruption is a core part of the OAIC's business. It is not an 'add on' or separate activity. All OAIC planning activities and plans are to consider the potential for fraud and corruption and implement proportionate countermeasures. This might include, for example, significant change projects that introduce new opportunities for fraud or reduce the effectiveness of existing controls.

Fraud and corruption control is to be incorporated into planning tools and templates where relevant.

The OAIC will report on its performance measures and its level of achievement in the Portfolio Budget Statements and its Annual Report.

Regulatory decision making

The OAIC exercises its powers honestly, impartially, transparently, for proper purposes and for the benefit of the community. The OAIC takes a contemporary approach to regulation by using data to assess risk and employing appropriate regulatory tools to address privacy and information access issues in a proportionate and evidence-based way.

The OAIC's responsibilities include conducting investigations, reviewing decisions and handling complaints. Our privacy and FOI regulatory action policies explain the OAIC's approach to using its regulatory powers. They are accompanied by a Guide to privacy regulatory action and Freedom of information guidelines issued under s 93A of the FOI Act. Staff are required to exercise the OAIC's powers within these parameters and are only able to exercise the delegations that have been set out in the Delegation Instrument issued by the Australian Information Commissioner.

The OAIC is committed to the development and retention of a highly skilled and professional workforce and reviews its regulatory approach to ensure that it aligns with government and public expectations.

Shared services and Whole of Government Panels

The OAIC utilises a number of shared services providers:

- Payroll and finance services provided by Service Delivery Office (SDO) within the Department of Finance
- ICT services provided by Department of Employment and Workplace Relations (DEWR).

Regular management meetings are held with each provider, including regular reporting to confirm metrics i.e., number of staff, user accounts and actioned services.

Whole of Australian Government purchases are via:

- Facilities management services provided by Ventia
- Real estate services provided by Colliers International

- Travel services acquired via QBT.

Protective security

The OAIC will seek regular assurance that appropriate security requirements outlined in the Commonwealth Protective Security Policy Framework (PSPF), Commonwealth Information Security Manual (ISM) and Department of Employment and Workplace Relations (DEWR) *IT Security Policy* are implemented and periodically evaluated for:

- **Physical security.** Accommodation, buildings and perimeters prevent the entry, exit and movement of unauthorised personnel, visitors and property
- **Information Security.** Sensitive and security classified material is afforded appropriate storage and protections, including during disposal
- **Personnel Security.** Recruitment of staff into designated security positions is undertaken in accordance with Commonwealth requirements.

The OAIC has a Security Framework that includes the following components:

- OAIC Security Policy Statement
- OAIC Threat and Security Risk Assessment and Implementation Plan
- OAIC Security Policy Manual
- OAIC Security Plan
- OAIC Security Procedures

Personnel services

The OAIC will seek regular assurance from its Director of People and Culture that:

Recruitment

- Recruitment policies and procedures ensure valid, fair, competitive recruitment actions in accordance with APS guidelines on merit recruitment.
- The classification, duties, responsibilities, authorities, lines of control and accountability, and any security clearances required for each position, are clearly specified for all positions, and included in duty statements, position profiles and organisational charts.
- Ensuring appropriate employment screening processes are in place.
- New staff sign a confidentiality and information security agreement.

Training and awareness

- Staff have been inducted upon commencement and supported throughout their probationary period with provision of fraud control information and advice.

- Induction training includes reference to OAIC policies on fraud and corruption prevention, and details of how staff can access them.
- Refresher and knowledge update training is provided on an ongoing basis. Staff with responsibility for fraud control and staff in high-risk fraud areas are provided with additional focused training.
- Fraud control and corruption training is part of a wider awareness campaign.
- Staff complete an annual attestation that they have understood and will comply with OAIC security and integrity requirements.

Payroll

- Payroll processes ensure timely, accurate, complete, and efficient processing of salary variations, allowances, entitlements and terminations in full compliance with the OAIC's Enterprise Agreement, *Public Service Act 1999* and *Public Service Regulations 2023* and related Commonwealth legislation.
- Payroll processes including adequate controls to minimise the risk of potential payroll related fraud events.
- Reports on staffing levels, staff-related payments, attendances, leave and absenteeism are regularly reviewed to identify and address anomalies or inconsistencies.

Leave and attendance

- The operation of the leave system is subject to regular reporting and review by the Director People and Culture to ensure compliance, accurate recording and reporting.

Performance management

- As required and agreed, managers' individual performance agreements contain performance measures and indicators relating to ethical behaviours in accordance with the APS Code of Conduct and APS Values.

Onboarding and Offboarding processes

- Upon commencement, staff complete a confidentiality and integrity declaration, acknowledging that they will comply with the OAIC Policies and Procedures, and the APS Code of Conduct and APS Values.
- Upon cessation, staff are required to sign the 'Acknowledgement of Continuing Obligations on Separation' form.

Conflict of interest and gifts and benefits

The OAIC will seek regular assurance that appropriate integrity requirements are implemented and periodically evaluated for the following:

- Reporting conflicts of interests – Under the OAIC Managing Conflicts of Interest Policy, all OAIC staff must provide a written declaration for any interests or conflicts, either actual or perceived, for themselves or immediate family members, that may be related to their OAIC employment.

- Reporting gifts and benefits – Under the OAIC Gifts and Benefits Policy, OAIC staff are required to report details of accepted gifts or benefits, and any gifts valued over $100 are to be registered in the Gift Register and published on the OAIC website.
- Reporting official hospitality – Under the OAIC Official Hospitality Guidelines, OAIC staff are required to obtain appropriate approval prior to providing or receiving official hospitality.

Financial management

Certain financial management services are provided to the OAIC under a shared services arrangement with the SDO.

The SDO must implement financial management practices to help:

- minimise the risk of fraud and/or corruption; and
- prevent and detect fraud and/or corruption.

The OAIC will seek regular assurance from the SDO, in respect of financial management practices that assist in minimising the risk of fraud and/or corruption, and preventing and detecting fraud and/or corruption, such as:

- The adequacy of financial management and reporting systems in respect of fraud prevention and detection, including:
  a) adequate segregation of duties and effective internal controls, including restrictions on system access
  b) adequate processing of all financial transactions
  c) adequate recording and reporting of financial transactions
  d) regular auditing by SDO with provision of reports to the OAIC.
- Financial services delivered to the OAIC fully comply with the PGPA Act and PGPA Rule, associated Commonwealth policies, Department of Finance advice and Estimates Memoranda, generally accepted public administration and government accounting principles and practices, Australian Equivalents to International Financial Reporting Standards and relevant management reporting requirements.

The OAIC will periodically review financial delegations and authorisations to ensure adequate segregation of duties.

Financial management will be monitored through the following key measures:

- monthly reconciliation between the OAIC's bank accounts and the financial management information system (FMIS), and between the payroll and FMIS.
- monthly examination by OAIC managers of budgeted revenue and expenditure against actual.
- internal and external audit.

Asset and property management

The OAIC will ensure timely, accurate, complete and efficient recording and processing of asset and property management transactions (in full compliance with the PGPA Act and PGPA Rule , associated Commonwealth policies, and applicable directions or guidance issued by the Department of Finance, and internal management control requirements) relating to:

a) contracting and acquisition

b) storage, issue, usage and return

c) maintenance and repair

d) retirement, disposal and write-off of assets and property

e) regular stock takes and asset reconciliations.

Facilities management services are provided to OAIC under a Whole of Australian Government arrangement. Ventia is OAIC's designated provider. Monthly management meetings are held to discuss provision of services and performance. OAIC reports bi-annually on Ventia's services to Department of Finance.

Information management and security

The OAIC will ensure that:

- Classified or sensitive information is managed in accordance with requirements contained in the Commonwealth Protective Security Policy Framework, the Cabinet Handbook, and any other relevant advice, including recording, monitoring and accounting for all movements of such documents and files.
- Classified material and records are periodically and systematically secured and reviewed for archival storage or disposal as appropriate.
- Non classified material and other internal records are managed in accordance with the OAIC *Information Management Policy*.

Information Technology (IT) services are provided to the OAIC by DEWR. The OAIC will seek regular assurance from DEWR that:

- arrangements, facilities, software and hardware comply with relevant Commonwealth and industry standards, including the PSPF.
- systems development methodologies, electronic communications security, change control procedures, and project management techniques are responsibly used in all new systems development, enhancement and modification.
- IT management functions are regularly monitored and evaluated.
- IT systems, controls and operations are periodically reviewed by IT management or an internal audit.
- specific aspects of IT functions are identified for extensive technical review by IT management or specialist external consultants from time to time.

Assurance Processes

Fraud control assurance processes for the OAIC include:

- the OAIC Internal Audit Strategic Work Plan
- external audit
- management initiated reviews

The assurance processes are implemented to test the effectiveness of the OAIC's fraud related controls, policies and procedures.

The Audit Committee provides independent assurance to the Australian Information Commissioner by overseeing and monitoring the adequacy of the fraud control arrangements and the processes and systems in place to capture and effectively investigate fraud related information. The Audit Committee and internal audit provider will ensure that:

- the planning and implementation of the internal audit program and audit techniques ensure appropriate and adequate coverage of all the OAIC's functions, procedures, systems and organisational arrangements over a rolling cycle
- audit programs are undertaken without improper executive influence or filtering
- working papers resulting from internal audits are kept
- audit techniques to assess the effectiveness of fraud control measures are integrated into the audit test program.

All aspects of the OAIC's activities will be accessible to the OAIC's internal and external auditors. The internal audit program will incorporate audit techniques to test systems for potential fraud, within the specific reviews Terms of Reference where appropriate to do so.

Public Interest Disclosure procedures

Public officials (disclosers) who suspect wrongdoing within the Commonwealth public sector can make a disclosure under the *Public Interest Disclosure Act 2013* (PID Act). Disclosures to the OAIC may be made in accordance with the OAIC's *Public interest disclosure procedures*.

The OAIC maintains a separate internal guide 'Investigation steps under the Public Interest Disclosure Act 2013' which provides a framework for:

- assessing disclosures that may fall within the PID scheme,
- allocating to the appropriate agency for investigation,
- steps to be undertaken in an investigation, and
- preparation of an investigation report.

It also incorporates detailed guidance on factors such as confidentiality, conflicts of interest, and communication with the discloser during the process.

All OAIC staff receive annual refresher training on the PID scheme and its requirements.

The PID Act offers protection to disclosers (‘whistle-blowers’) from reprisal action and requires that specific steps are taken to assess the risk of reprisal to disclosers.

Fraud Risk Assessment

The OAIC performs an overall business level Fraud Risk Assessment on a (not less than) two-yearly basis. This Fraud Risk Assessment assesses fraud and corruption risks at a more granular level for typical risk types and sources. The Fraud Risk Assessment is organised under the following categories:

1. Allowances
2. Purchasing and accounts payable
3. Corporate credit/charge cards
4. Information security (non-IT)
5. Information technology security
6. Salaries and personnel
7. Property
8. Cash and banking
9. Fraud awareness
10. OAIC regulatory and operational decision making
11. Performance reporting
12. Use of position.

An ongoing monitoring program is coordinated by the Director, Governance and Risk and Chief Risk Officer, in collaboration with individual risk stewards and subject matter experts, to review 1-2 fraud and corruption related risks in each of the above categories from the Fraud Risk Assessment each month. Risks identified for review are prioritised on the basis of their residual risk rating, effectiveness of current controls and whether the risk is currently acceptable to the OAIC.

The Fraud Risk Assessment identifies specific fraud and corruption risks in each of these categories. For each risk it also assesses and describes:

- A steward for each risk to ensure its proactive monitoring and management.
- Potential causes and sources. This includes mechanisms or pathways by which the fraud event could be realised.
- The potential consequences should the fraud risk event be realised.
- Controls currently in place to detect, prevent or mitigate the fraud risk event. This includes controls implemented by the OAIC or its supporting partners.
- An assessment of the effectiveness of these controls.
- An assessment of the current likelihood, potential consequence, and severity.
- An assessment of the current acceptability of this level of risk.

- Any new controls or treatment that are required to be implemented to make the risk acceptable.

The assessment of these fraud and corruption risks is consistent with the OAIC's *Risk Management Policy and Framework*.

The Fraud Risk Assessment is maintained by the Assistant Commissioner, Corporate. Due to the nature of the potential vulnerabilities described in the assessment, distribution of the document is controlled.

Risks identified within the Fraud Risk Assessment, are to be reviewed and 'pressure tested' each not less than every twelve months. This process is to include a full walk-through of the risk, followed by collaborative challenge and debate.

Risk Control Testing

The OAIC should continue to monitor and test the operating effectiveness of the specific fraud and corruption risk controls to ensure that they continue to meet both the current and emerging risks faced by the agency. An annual fraud and corruption risk control testing implementation plan should be developed by the Director, Governance and Risk and approved by the Chief Risk Officer. This plan should detail the timeframes and priorities for individual risk controls to be tested based on the residual risk rating for the risk, prior effectiveness of the risk control and whether the risk is currently acceptable to the OAIC.

The following should be recorded in the Fraud and Corruption Risk Control Report as evidence of the outcomes from the risk control testing:

- Details of the current control
- Whether the control is preventative, detective or corrective
- Evidence that will be used to assess the control, for example, audit, user testing
- Rating of the effectiveness of the control [Effective, Partially Effective, Ineffective]
- Description of how the control effectiveness rating, for example, 'controls are in place but could be strengthened'
- Details of any evidence relied upon to make the assessment
- Any future treatments that are identified as necessary as part of the testing
- Timeframes for the implementation of any future treatments.

Appendix A. Fraud Risk Assessment

A copy of the Fraud Risk Assessment can be obtained by contacting the Assistant Commissioner Corporate.

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]

s47E(a), S47E(c), s47E(d)

[redacted]