

Fraud and Corruption Control Policy

November 2022



contents

1	Policy statement	1
2	Objective	1
3	Scope	1
4	Fraud and corruption control system	1
4.1	Attribute one: Leadership	2
4.2	Attribute two: Ethical framework	2
4.3	Attribute three: Responsibility structures	2
4.4	Attribute four: Fraud and corruption control policy	4
4.5	Attribute five: Fraud and corruption risk management	4
4.6	Attribute six: Prevention systems	5
4.7	Attribute seven: Awareness	6
4.8	Attribute eight: Third party management systems	7
4.9	Attribute nine: Notification systems	7
4.10	Attribute ten: Detection systems	8
4.11	Attribute eleven: Investigation systems	9
4.12	Attribute twelve: Breaches	10
4.13	Attribute thirteen: Recovery and review	10
5	Legislative context	11
6	Definitions	11
7	Contact point	12
8	Review	12

1 Policy statement

The Audit Office of New South Wales (the Audit Office) is committed to embedding an honest and ethical environment that minimises the risk of fraud and corruption.

Fraud and corruption are incompatible with the Audit Office’s values and the Code of Conduct and can cause serious reputational damage. For these reasons the Audit Office has zero tolerance to fraud and corruption.

Acts or behaviours leading to fraud and corruption are considered a breach of this Policy and the Code of Conduct and may result in disciplinary action in accordance with the Audit Office’s Disciplinary Policy or action against a third party. Any fraud or corruption that is detected may also be reported to a relevant law enforcement agency.

2 Objective

This Policy establishes a fraud and corruption control system (FCCS) consistent with the Australian Standard on Fraud and Corruption Control (AS 8001:2021) and the NSW Fraud and Corruption Policy (TC 18-02). This Policy provides guidance on how to prevent, detect and respond to incidents of fraud and corruption by:

- reinforcing management’s commitment to, and responsibility for, managing fraud and corruption risk, and ensuring all Staff¹ are aware that the Audit Office has zero tolerance for fraud or corruption
- requiring Staff to perform their duties with honesty and integrity in accordance with the Ethical and Lawful Framework that underpins the expected standards of behaviour for all Staff
- protecting the reputation and assets of the Audit Office from fraud and corruption.

3 Scope

This Policy applies to all Staff (refer to the definitions in section 6 of this Policy).

This Policy should be read in conjunction with the Code of Conduct and other related policies and procedures including those forming part of the Ethical and Lawful Framework and Employee Conduct and Obligations pages of our intranet.

4 Fraud and corruption control system

The Audit Office’s approach to fraud and corruption control is based on 13 key attributes within the themes of prevention, detection and response, which together make up the Audit Office’s FCCS:



¹ Refer to the Definitions in section 6 of this Policy.

The FCCS will be regularly reviewed and amended considering:

- outcomes of regular risk assessments
- historical incidents or behaviours of fraud and corruption
- changes in internal and external circumstances, developments, and trends identified through environmental scans
- better practice and guidance from relevant organisations including from the Independent Commission Against Corruption (ICAC)
- changes in relevant legislation.

4.1 Attribute one: Leadership

The Audit Office's FCCS is led by the Auditor-General with the support of the Office Executive and the Governance Unit, who together accept and acknowledge accountability in preventing and managing the Audit Office's fraud and corruption risks.

This is shown by a commitment to:

- modelling the highest standards of ethical behaviour
- not tolerating fraudulent or corrupt behaviour
- providing adequate support and resources to implement the FCCS
- requiring all Staff to be aware that fraud and corruption prevention is the responsibility of everyone within their area of responsibility, supported by a training and awareness program
- treating all complaints and incidents of fraud and corruption seriously
- taking fair and proportionate action against Staff or a third party found to have engaged in fraud and corruption.

4.2 Attribute two: Ethical framework

The Audit Office has clear policies setting out acceptable standards of ethical behaviour and these are available to Staff within the Ethical and Lawful Framework and Employee Conduct and Obligations pages on the intranet. These policies are reviewed regularly to ensure they are up to date and in line with the Audit Office's compliance obligations.

Staff are required to evidence their commitment to acceptable standards of ethical behaviour by annually acknowledging the Code of Conduct and submitting a Conflict of Interest and Professional Independence Declaration.

4.3 Attribute three: Responsibility structures

4.3.1 Responsibilities within the Audit Office

Auditor-General has ultimate responsibility for the FCCS and ensuring that the Audit Office has in place adequate anti-fraud and anti-corruption measures. The Auditor-General also has responsibilities under other acts in relation to fraud and corruption, namely under the *Independent Commission Against Corruption Act 1988* (ICAC Act), *Public Interest Disclosures Act 1994* and *Law Enforcement Conduct Commission Act 2016*.

Office Executive is responsible for:

- supporting the Auditor-General in committing to and implementing the FCCS, including as outlined in section 4.1
- approving this Policy
- considering fraud and corruption when making business decisions including approving Audit Office's policies, procedures, practices, systems and business plans.

Leadership Team is responsible for:

- promptly reporting fraud and corruption matters that come to their attention, in accordance with section 4.9
- being aware of and managing fraud and corruption risks within their area of responsibility and ensuring fraud and corruption controls are operating effectively
- ensuring Staff complete assigned training and are aware of fraud and corruption risks.

All Staff:

- are responsible for preventing and controlling fraud and corruption within their area of responsibility
- be aware that fraud and corruption may occur within their area of responsibility
- must comply with the Code of Conduct and other policies within the Ethical and Lawful Framework and Employee Conduct and Obligations on the intranet
- are expected to cooperate with all initiatives aimed at preventing, detecting and responding to fraud and corruption, such as completing Staff questionnaires or surveys, input into risk assessments, completing related training and education, etc
- must report known or suspected fraud and corruption or matters that raise fraud and corruption risk as soon as possible, in accordance with section 4.9.

4.3.2 Specialist roles

Executive Director, Professional Services has a central role in dealing with reports made by Staff and:

- oversees the implementation of the Audit Office's FCCS
- advises the Auditor-General, Deputy Auditor-General and Director, Human Resources of allegations of fraud and corruption
- escalates matters relating to fraud and corruption in accordance with section 4.9.

Director, Governance (Risk and Ethics):

- leads the development, implementation, and review of the Audit Office's FCCS and the various activities as outlined in the Fraud and Corruption Control Plan (the F&C Control Plan)
- coordinates periodic assessments of the Audit Office's fraud and corruption risks and reports the results to the Office Executive and the Audit and Risk Committee
- ensures fraud and corruption events are recorded in the Fraud and Corruption Event Register as outlined in section 4.13.2
- is authorised to receive reports of fraud and corruption, escalates reports in accordance with section 4.9 including coordinating internal and external reporting to relevant law enforcement agencies as required
- conducts, coordinates, and monitors assessments or investigations into allegations of fraud and corruption, ensuring they are conducted thoroughly and objectively
- oversees the implementation of fraud and corruption control training and awareness
- regularly reports to the Office Executive and Audit and Risk Committee on the FCCS and details of any fraud and corruption investigations conducted during the year
- attends continuing professional development to maintain awareness of best practice in managing the risk of fraud and corruption.

Director, Human Resources is responsible for:

- ensuring the welfare of Staff involved in an allegation of fraud or corruption
- managing any breaches of conduct and behaviour in line with the Audit Office's Disciplinary Policy

- developing and implementing effective employment screening and recruitment and selection policies and processes.

Chief Information Officer is to:

- have a sound understanding:
 - of any technology enabled fraud and corruption exposures
 - how an Information Security Management System (ISMS) can effectively mitigate the risks of fraud and corruption
 - of cybercrime and the methods for managing the risks of cybercrime
- assist in the capture and analysis of digital evidence in the event of any investigation following a report of a fraud and corruption incident.

Chief Audit Executive and Internal Audit Function assist in preventing fraud and corruption by:

- examining and evaluating the adequacy and effectiveness of internal controls
- in consultation with the Chief Risk Officer (CRO), developing a risk based internal audit program that considers inherently high-risk fraud and corruption areas, functions or activities
- reporting fraud and corruption incidents or elevated risk as soon as it is detected
- periodically reviewing the effectiveness of the FCCS, including this Policy.

Internal audit is not specifically responsible for detecting fraud and corruption but is expected to be alert to and consider the Audit Office's exposure to fraud and corruption and provide assurance on internal controls.

4.3.3 Audit and Risk Committee responsibilities

The Audit and Risk Committee provides independent assistance and advice to the Auditor-General in accordance with its Charter.

The Committee is responsible for review of the FCCS including F&C Control Plan and ensuring the Audit Office has appropriate processes and systems in place to capture and effectively investigate fraud and corruption related information.

4.4 Attribute four: Fraud and corruption control policy

This Policy provides guidance on how to control fraud and corruption and covers the responsibilities for managing fraud and corruption within the Audit Office. It does not operate in isolation and has strong links to various Audit Office's policies including but not limited to:

- Code of Conduct
- Statement of Business Ethics
- other policies forming part of the Ethical and Lawful Framework and Employee Conduct and Obligations pages of intranet.

4.5 Attribute five: Fraud and corruption risk management

Fraud and corruption risk is managed in line with the requirements of the Audit Office's Risk Management Framework².

² The Audit Office's risk management framework is developed and maintained in line with the Management Toolkit for NSW Public Sector Agencies (TPP 12-03) and the AS/NZS 31000:2018 Risk Management - Guidelines, which provide guidance to agencies on the development of effective and integrated risk management frameworks and processes.

A formal, overarching fraud and corruption risk assessment is led by the CRO, and conducted at least every two years or sooner if required (including an informal review every other year). The risk assessment will consider both internal and external factors.

The results of the overarching fraud and corruption risk assessment will:

- inform the development of the Audit Office's F&C Control Plan so it focuses on areas of greatest exposure
- identify corrective actions or additional controls to remedy any unacceptable risks
- be reported to the Office Executive and Audit and Risk Committee

In addition to the overarching risk assessment, targeted risk assessments will also be conducted within business functions, activities or projects that have an inherently higher risk of fraud and corruption (e.g. procurement and contract management or purchasing and accounts payable). This should be conducted by those responsible for the specific functions, activities or projects including when developing and implementing policies, procedures, systems, controls, etc.

If management and Staff are unsure about assessing and managing fraud and corruption risks for their respective areas, they should contact the CRO.

4.6 Attribute six: Prevention systems

The Audit Office's prevention systems contain a number of components including:

4.6.1 F&C Control Plan

The F&C Control Plan outlines the Audit Office's approach and activities to controlling fraud and corruption exposures. It is a risk-based plan that includes 'pressure testing' the FCCS by an internal or external party, who initiates a series of transactions to assess the operational effectiveness of internal controls.

4.6.2 Ethical workforce

The Audit Office is committed to employing Staff who align with and support the Audit Office's values.

The Audit Office's Recruitment and Selection Policy aims to recruit and promote the most suitable person for a role based on merit and through selection decisions that are consistently and equitably applied. Selection panel members are required to disclose any conflicts.

The Audit Office's Employment Screening Policy outlines requirements for pre-employment and existing employment screening which is effective in reducing the Audit Office's exposure to fraud and corruption.

4.6.3 IT security

The Audit Office's FCCS is reliant on the organisation wide approach to managing information and cyber security risks and draws on the benefits of the Audit Office's ISMS.

The Audit Office's ISMS outlines the suite of policies, procedures and controls taken by the Audit Office to manage information and cyber security risks which in turn supports the prevention, detection and response to technology enabled fraud and corruption. The ISMS Framework is consistent with and certified against the AS ISO/IEC 27001 Information technology – Security techniques – Information Security Management Systems and in line with the NSW Cyber Security Policy.

4.6.4 Physical security

The Audit Office must implement appropriate measures to prevent the theft of valuable tangible assets. This will be done in accordance with the Audit Office's Physical Security Policy and may include access controls, identity and visitor cards and panic alarms.

4.6.5 Managing conflicts of interest and threats to professional independence

Conflicts of interest and threats to professional independence arise when personal interests conflict with the duty to act in the public interest or as an independent integrity agency. Fraud and corruption may occur because a conflict of interest has been concealed, understated or mismanaged. Identifying and managing conflicts of interest or threats to professional independence is effective in reducing the exposure to fraud and corruption.

Refer to the Audit Office's Conflict of Interest and Professional Independence Policy.

4.6.6 Managing gifts, benefits and hospitality

Accepting gifts, benefits or hospitality has the potential to compromise Staff by creating a sense of obligation and undermining their impartiality. Staff must be open and transparent about offers of gifts, benefits, or hospitality in line with the Audit Office's Gifts, Benefits and Hospitality Policy.

4.7 Attribute seven: Awareness

4.7.1 Staff awareness

Staff need to understand fraud and corruption is not tolerated and the possible consequences of committing fraud and corruption. They need to be aware of:

- what is fraud and corruption
- common types of fraud and corruption they may encounter or red flags to be aware of
- their responsibilities
- how to report suspected fraud and corruption
- an overview of the Audit Office's FCCS.

The details of the Staff awareness program are outlined in the Audit Office's F&C Control Plan and include:

- induction and post induction training
- specialised training targeted to those working in inherently higher risk areas
- policies and procedures available to all Staff on the intranet
- notifications and Staff reminders as required
- annual Staff Conflict of Interest and Professional Independence declarations
- annual attestations to the Code of Conduct.

4.7.2 External stakeholder awareness

External stakeholders also need to understand fraud and corruption is not tolerated and the possible consequences of committing fraud and corruption.

External stakeholders include:

- Parliament of New South Wales
- citizens and the community
- auditees and staff within the public sector
- third parties who work for and on behalf of the Audit Office (as outlined in the Statement of Business Ethics), including Audit Service Providers (ASPs), suppliers, technology partners, consultants, contractors, etc.

The Audit Office ensures awareness by:

- making relevant documents and policies available on the Audit Office's website including this Policy and the Statement of Business Ethics
- clearly stating obligations in tender documents, contracts, and other related documents

- conducting awareness workshops and issuing reminders to relevant third parties including ASPs.

4.8 Attribute eight: Third party management systems

The Audit Office ensures specific internal controls are in place to manage our dealings with third parties including preventing fraud and corruption by third parties against the Audit Office which includes:

- ensuring third parties are aware of, understand and comply with the Statement of Business Ethics as outlined in section 4.7.2
- commitment to complying with [PBD-2017- 07 Procurement Board Direction - Conduct by Suppliers](#) and reporting dishonest, unfair, unconscionable, corrupt or illegal conduct
- requiring certain third parties to report any conflicts of interest and gifts and benefits offered that may affect the independence of the Auditor-General as outlined in contractual obligations
- conducting third party security risk assessment in line with the Third Party Security Policy, prior to engaging with third parties and requesting third parties adopt minimum security requirements
- outlining obligations in contracts or other relevant documents including the ASP Manual
- requiring annual declarations by relevant third parties
- third party vetting and due diligence as part of procurement process.

4.9 Attribute nine: Notification systems

4.9.1 Reports from Staff

If a staff member knows or reasonably suspects:

- another staff member has acted fraudulently or corruptly
- another organisation or person has acted fraudulently or corruptly against the Audit Office
- there is suspicious fraudulent or corrupt activity including cyber fraud or
- heightened risk of fraud and corruption not being adequately managed

they must report it as soon as possible to the following:

- Director, Governance (Risk and Ethics)
- Executive Director, Professional Services.

For guidance on how to report suspected or actual fraud and corruption refer to the Internal Public Interest Disclosures Policy (Internal PID Policy).

Staff can discuss their concerns in the first instance with their people manager or those outlined above. Staff are encouraged to make a report in writing, as this helps to avoid any confusion or misinterpretation.

Staff are to be aware of the provision in section 316(1) of the *Crimes Act 1900* which says that a failure to report a serious offence is an offence.

The Audit Office will not tolerate any reprisal action against Staff who report known or suspected incidents of fraud and corruption and will ensure appropriate action is taken to protect the Reporter (refer to the Definitions in section 6 of this Policy). The Internal PID Policy includes further details about the protections against reprisals available to Staff and what to do if they believe detrimental action has been or is being taken against them.

The Audit Office will make sure that Reporters are supported and encouraged to access the professional support services they may need as a result of the reporting process – such as stress management, counselling services or legal advice.

4.9.2 Reports from external stakeholders

External stakeholders (as outlined in section 4.7.2) are encouraged to report suspected or actual cases of fraud, misconduct or unethical behaviour by Audit Office Staff. Refer to the Audit Office's website page 'Make a complaint about us'.

Individuals employed within the public sector (including third parties who work for and on behalf of public sector entities) can also refer to the External Public Interest Disclosure Policy.

4.9.3 Notifying law enforcement agencies and ICAC

If Staff have concerns that their report to management will not be dealt with appropriately then they have the option of reporting directly to the ICAC.

Where, on reasonable grounds, there is suspicion that corrupt conduct has occurred, the Auditor-General has a duty under section 11 of the ICAC Act to report it to the ICAC as soon as the suspicion arises. This is irrespective of how insignificant or minor the allegation is.

Additionally, fraud and corruption may be referred by the Auditor-General to other relevant external bodies such as the NSW Police Force, the Crown Solicitor, the Director of Public Prosecutions, or the NSW Ombudsman as appropriate and in line with legislation.

4.9.4 Notifying affected third parties of data breaches

The Audit Office's Data Breach Management Policy outlines the requirements to notify third parties to reduce the risk of fraud and corruption.

4.10 Attribute ten: Detection systems

The Audit Office is committed to establishing robust systems of detection. This is done through a set of processes including:

- post transactional review
- analysis of management accounting reports
- identification of early warning signs
- data analytics
- fraud and corruption reporting channels
- whistleblower protection
- leveraging relationships with business associates and other external parties
- complaint management
- exit interviews.

4.10.1 Detection by internal and external audit

It is not the responsibility of internal or external audit to specifically identify fraud and corruption risk. However, in testing controls and past transactions they may be able to detect actual or suspected incidents of fraud and corruption, in which case they are required to notify the Audit Office. Common techniques used by internal and external audit such as data mining, data analytics, and post transactional reviews, may detect fraud or corruption.

4.10.2 Financial and non-financial analysis

The Audit Office will have in place processes to review financial reports to detect anomalies that may be indicative of fraud or corrupt conduct. Such analysis may include:

- monthly actual/budget/prior period comparison reports
- industry benchmarking
- reports highlighting unusual trends in bad or doubtful debts, time records, leave balances, etc.

4.10.3 IT and system detection

The Audit Office's ISMS Framework (as noted in section 4.6.3) also outlines the suite of policies, procedures and controls taken by the Audit Office which can detect fraud and corruption resulting from information and cyber security incidents. Detection controls may include vulnerability scanning, review of access logs or checking privilege access.

4.10.4 Internal and external complaints and PIDs management

The Audit Office values feedback to improve its operations on an ongoing basis. Complaints, compliments, or suggestions are encouraged from internal and external stakeholders. The Audit Office reviews the nature and types of complaints to identify trends or spikes that may indicate fraud or corruption.

Refer to section 4.9.1 on how Staff can make a report.

Refer to section 4.9.2 on how external stakeholders can make a report.

4.10.5 Exit interviews

Exit interviews are conducted for terminated Staff and will be open to identifying any red flags or relevant information about possible fraudulent and corrupt events.

4.11 Attribute eleven: Investigation systems

4.11.1 Preliminary assessment

When a Reporter makes an allegation of fraud or corruption against a Subject Staff Member (refer to the Definitions in section 6 of this Policy), the Director, Governance (Risk and Ethics), Executive Director, Professional Services, the Director, Human Resources, Deputy Auditor-General or the Auditor-General will discuss the matter with the Reporter. The Reporter may be asked to make a written statement regarding the allegations.

The Subject Staff Member may be interviewed during this preliminary stage and can be accompanied by their people manager or other nominated support person during the interview.

The Director, Governance (Risk and Ethics):

- will aim to acknowledge the report of fraud or corruption within ten working days and no later than 45 working days of receipt, providing the name and contact details of the people who can provide further updates or information
- will organise a preliminary assessment of the allegations and provide appropriate details to the Reporter of any decisions and how the allegations will be progressed
- may recommend to the Auditor-General that the matter be immediately referred to an external body. A full investigation may still be undertaken even through another agency, such as the NSW Police Force or the ICAC, is also investigating.

4.11.2 Full investigation

Following the preliminary assessment, the Director, Governance (Risk and Ethics) may recommend to the Auditor-General a full investigation be conducted by an appropriately qualified external investigator. Any internal investigation will be conducted in accordance with the ICAC's [Factfinder – A guide to conducting internal investigations](#) (April 2022) where considered appropriate.

The Reporter will be advised of the decision and any actions that will be taken. When further action is to be taken, the Subject Staff Member may also be notified.

4.11.3 Maintaining confidentiality

The Audit Office will take all possible steps to ensure that any allegations of fraud or corruption and subsequent investigations are handled confidentially. This is designed to help prevent any action

being taken against Reporters. However, there may be situations where confidentiality may not be possible or appropriate. This will be discussed with the Reporter.

While anonymous reports are not encouraged, there may be situations where someone may not want to identify themselves. The Audit Office will accept anonymous reports, however anonymity may limit our ability to seek further information to assess the report adequately. When the identity of the Reporter is known, the Audit Office is able to obtain any further necessary information, provide the Reporter with protection and support and give feedback about the outcome of any investigation into the allegations.

4.11.4 Other considerations when investigating

During any investigation, the Director, Human Resources will be involved to ensure the Disciplinary Policy is properly followed and that any personnel issues affecting the staff members involved are properly addressed.

Proper and full records must be kept during the investigation and any evidence gathered (physical or digital) will be secured and preserved.

The results of any investigation will be reported to the Auditor-General, Office Executive and Audit and Risk Committee.

Investigations can put the investigators at personal risk including the risk of physical, emotional and psychological harm. Following the discovery of a fraud and corruption event, the Audit Office will assess the risk and ensure safety of the investigators.

In order to ensure an adequate investigation and response is taken and that crucial evidence is preserved, the Audit Office will take immediate action in response to discovery of a fraud and corruption event, including documenting how the event was identified, and the considerations, actions and assessments taken.

4.12 Attribute twelve: Breaches

4.12.1 Disciplinary actions for Staff

Where the allegation is proved because of an admission by the Staff or as a result of an investigation, the Director, Governance (Risk and Ethics) and the Director, Human Resources will make a recommendation to the Auditor-General and/or Deputy Auditor-General regarding disciplinary action or referral to an external body.

The Deputy Auditor-General and/or Auditor-General will determine the nature of any disciplinary action.

The disciplinary process as outlined in the Audit Office's Disciplinary Policy must be followed.

4.12.2 Consequences for third parties

In accordance with the Statement of Business Ethics, non-compliance to the statement including perpetrating fraud and corruption against the Audit Office, could lead to termination of contracts, loss of future work, matters being referred for criminal investigation or to a relevant law enforcement agency or other action as considered appropriate.

4.13 Attribute thirteen: Recovery and review

Where appropriate, the Audit Office may seek to recover any losses including lodgement of a claim against the Audit Office's insurance policy.

Following each instance of fraud and corruption found, the internal control environment will need to be reassessed and consider whether remediation or enhancements are required.

4.13.1 Making vexatious, frivolous or misleading allegations

Any report that turns out to be vexatious, frivolous or misleading will result in disciplinary action against the Reporter.

4.13.2 Fraud and corruption event register (the Register)

The Director, Governance (Risk and Ethics) will maintain the Register of all reports of suspected or actual fraud and corruption. The Register will help the Audit Office determine where to focus its efforts and where changes to controls, policies or procedures are required. The Register records all incidents of fraud and corruption affecting the Audit Office, including actions taken and the outcomes.

5 Legislative context

This Policy has been developed with reference to:

- [AS 8001-2021 Fraud and Corruption Control](#) (AS 8001-2021)
- the Audit Office's [Fraud Control Improvement Kit](#), February 2015
- AS ISO 37001-2019 Anti-bribery Management Systems (AS/ISO 37001: 2019)
- AS/NZS ISO 31000 Risk management – Guidelines
- AS ISO/IEC 27001 Information technology – Security techniques – Information Security Management Systems
- [Treasury Circular TC 18-02 – NSW Fraud and Corruption Control Policy](#)
- [IIA Whitepaper – Corruption-related risks in decision making](#)
- [IIA Whitepaper – Fraud and Corruption Risk Assessments](#)
- ICAC's [Factfinder – A guide to conducting internal investigations](#), April 2022
- ICAC's [Corruption and Integrity in the NSW Public Sector: an assessment of current trends and events](#), December 2018
- ICAC's [Strengthening Employment Screening Practices in the NSW Public Sector](#), February 2018
- *Public Interest Disclosures Act 1994*
- *Independent Commission Against Corruption Act 1988*
- *Government Sector Finance Act 2018*.

6 Definitions

Bribe/Bribery³: offering, promising, giving, accepting or soliciting of an undue advantage of any value (which could be financial or non-financial), directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to performance of that person's duties.

Corruption⁴: a dishonest activity in which a member of Audit Office Staff acts contrary to the interests of the Audit Office and abuses their position of trust in order to achieve personal advantage or advantage for another person or organisation. This can also involve corrupt conduct by the Audit Office, or a person purporting to act on behalf of and in the interests of the Audit Office, in order to secure some form of improper advantage for the Audit Office either directly or indirectly.

³ Source: [AS/ISO 37001: 2019](#).

⁴ Source: AS 8001-2021.

The concept of corruption in AS 8001-2021 is broader than the concept of bribe or bribery in [AS/ISO 37001: 2019](#). All acts of bribery would constitute corruption under AS 8001-2021 but not all acts of corruption would constitute bribery under [AS/ISO 37001: 2019](#).

While conduct must be dishonest for it to meet the definition of corruption, the conduct does not necessarily represent a breach of the law.

Fraud⁵: a dishonest activity causing actual or potential gain or loss to the Audit Office, including theft of moneys or other property by employees or persons external to the Audit Office and/or where deception is used at the time, immediately following the activity. This also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit.

While conduct must be dishonest for it to meet the definition of fraud, the conduct need not necessarily represent a breach of criminal law.

Reporter means staff member who reports suspected fraud or corruption.

Subject staff member means Staff against whom the allegations of fraud or corruption are made.

Staff means all permanent and temporary staff and the contingent workforce employed by the Audit Office.

7 Contact point

The contact for this Policy is the Director, Governance (Risk and Ethics). See section 4.9 of this Policy on how to report suspected or actual fraud, corruption or unethical behaviour.

8 Review

The Policy will be reviewed at least every three years in the absence of any significant changes or more frequently where required, taking into account legislative or organisational change, risk factors and consistency with other supporting policies.

⁵ Source: AS 8001-2021.