



Oifig an Ard-Reachtaire Cuntas agus Ciste
Office of the Comptroller and Auditor General

Anti-fraud policy

Contents	Page
1. Purpose	3
2. Policy statement	3
3. General principles	4
4. Definition of fraud	4
5. Fraud risk areas	5
6. Internal controls	7
7. Anti-fraud responsibilities	8
8. Penalties	11
9. Reporting fraud	11
10. Lessons learned	13
11. Policy review and approval	13
12. Policy acceptance by staff	13

1. Purpose

The Office of the Comptroller and Auditor General (the Office) and its Audit Board are firmly committed to a zero-tolerance approach in relation to bribery, corruption and fraud. The Office seeks to promote an anti-fraud culture and an ethos for all staff in which raising concerns and speaking up is valued, in situations where there is a reasonable belief that wrongdoing is taking place.

The purpose of this policy is to:

- provide a definition of fraud
- give guidance to staff on their duties and responsibilities in connection with fraud and suspected cases of fraud in relation to the Office's income, expenditure, assets and liabilities
- outline the steps and safeguards whereby staff may, in confidence, raise concerns regarding suspected or actual fraudulent activity
- set out the statutory protections for staff raising such concerns and the Office's internal procedures for dealing with disclosures.

As an integral component of a good control environment in the Office, it is essential that all staff be aware of the possibility of fraud and be conscious of their duties and responsibilities to prevent it. Given the nature of the work of the Office the impact of any instances or allegations of fraud might not be limited to financial loss but could also potentially diminish the reputation of the Office.

2. Policy statement

To give assurance to the public and to the Office's other stakeholders the Office must have a clear statement of its anti-fraud policy and the protection for staff reporting fraud or suspected fraud. This statement is as follows:

*The Office of the Comptroller and Auditor General and its Audit Board operate a **zero-tolerance** attitude to fraud. It requires staff and senior management at all times to act honestly and with integrity, to safeguard public resources for which they are responsible and to report suspicions of fraud.*

The Office acts to prevent fraud, in relation to moneys and assets for which it is responsible, through:

- *openness, transparency and accountability in its policies and procedures*
- *carrying out risk managed reviews, and regular monitoring of activities and functions*
- *ensuring all staff are aware of their obligations and*
- *segregation of duties, strict adherence to approval limits, restricted access to payment mechanisms, internal audit and maintaining an asset register.*

All staff are encouraged to raise genuine concerns regarding improprieties in the conduct of the Office's activities, whether in matters of financial management or other malpractices, at the earliest opportunity and in an appropriate way.

The Office recognises and supports staff who raise genuine concerns. You will not be disadvantaged for speaking up about a concern, provided you reasonably believe the allegations to be true. All concerns will be treated fairly and properly.

3. General principles

In accordance with best practice, the Office has an obligation:

- to prevent fraud and to have systems designed to prevent it
- not to engage in fraud
- to have systems designed to detect fraud if it has occurred or is occurring
- to report fraud if it does occur
- to deal with fraud if detected or reported
- to act to recover any losses occurring because of fraud.

The Office is committed to preventing fraud from occurring and to fostering an appropriate culture to avoid such events. To ensure these objectives are achieved:

- All Office staff must have, and be seen to have, the highest standards of propriety and honesty in the exercise of their duties
- The Office will not tolerate fraud, dishonesty, or impropriety
- The Office takes steps to identify, evaluate and address the potential for fraud either from persons or groups outside the Office or from within the organisation
- All instances of fraud or suspected fraud will be reported to senior management, the internal and external auditors and the Audit Committee
- The Office will investigate promptly all allegations of fraud and will take appropriate action (see section 8 – 'Penalties').

4. Definition of fraud

Fraud means dishonest and or illegal acts that result in loss or intended loss, whether financial or otherwise, to the Office. Fraud can be committed at all levels within the organisation, from higher financial transactions to routine activities.

For practical purposes fraud can be defined as the use of deception with the intention of obtaining an advantage, avoiding an obligation or causing loss to another party. The criminal act is the attempt to deceive, and attempted fraud is, therefore, treated as seriously as accomplished fraud.

Fraud occurs in a variety of ways. Inevitably it involves the misappropriation of funds or assets of the Office. Frauds can include:

- payment fraud
- presenting unsolicited invoices to be paid by the Office
- presentation of forged or falsified documents
- misappropriation or misuse of assets/consumable items
- false accounting or making fraudulent claims with a view to personal gain
- bribery and corruption
- ICT/cyber fraud (see '(v) ICT systems/cyberattack' in section 5 – 'Fraud risk areas').

Who carries out fraud?

Fraud may be carried out by:

- an individual/group outside the Office, including an organised criminal group e.g. cybercriminals
- an individual/group inside the Office
- collusion between individuals or groups inside and outside the Office.

5. Fraud risk areas

Five broad categories of risk need to be examined in pursuing fraud prevention. These are **(i) staff, (ii) external, (iii) physical/operational, (iv) financial and (v) ICT systems/cyberattack.**

(i) Staff

All staff should practice high standards of behaviour at all times. Staff shall not engage in outside employment or business without prior approval of the Secretary.

Everyone should be aware of common signs indicating possible fraudulent behaviour. While common signs should not, on their own, be considered suspect, matters such as behaviour, performance and attendance should be regularly monitored by supervisors and management.

Common signs can include:

- staff refusing to take holidays
- staff who keep responsibility for functions which they could easily delegate or train others to do
- staff who obtain full control of an area of work
- staff who engage in outside employment or business while working remotely or while on paid sick leave without the knowledge of the Office.

(ii) External

External risks are associated with external agencies including suppliers of services, contractors working on behalf of the Office, competing firms and audit bodies. The nature of the fraud risks in this context include bribery and profiting or seeking to profit from third parties by virtue of official position or duties. Such risks may arise in relation to the procurement of goods and services by the Office.

The Office has controls in place in relation to its procurement procedures, including segregation of duties and management oversight.

The European Single Procurement Document, which must be completed in respect of tenders advertised on eTenders, outlines exclusion grounds for the award of new contracts which relate to convictions for; participation in a criminal organisation, corruption, fraud, terrorist offences or offences linked to terrorist activities, money laundering or terrorist financing, child labour and other forms of trafficking in human beings.

(iii) Physical/operational

The Office reviews physical access controls as part of its fraud prevention procedures. Restricting access to cash, goods, stores, electronic payment systems, and official documents and premises is a critical element in reducing the risk of fraud.

(iv) Financial

The Office's financial operations can at any time be at risk to fraud. The scale of risk is likely to be related to:

- the amount of money involved
- the complexity of the process
- the frequency and effectiveness of Office controls.

The Office has in place a system of internal financial control to mitigate such risks including an annual review of its effectiveness.

(v) ICT systems/cyberattack

ICT systems can be used to carry out frauds which were formerly carried out manually e.g. falsely authorising a payment. There are some technical frauds where ICT skills are used as the primary mechanism for executing the fraud. It is essential that all staff, especially managers, have an understanding of the information technology in use in their area of work.

The ability to install or change ICT software is strictly controlled. System access is managed and controlled in accordance with the *Office Access Control policy* and using the *movers and leavers procedures* when a staff member moves team or when a staff member leaves the Office.

The Office seeks to minimise the risk of ICT fraud by, inter alia, periodic review of ICT controls by the Office's internal audit function and ensuring its information security management system continues to meet the requirements of ISO 27001. Senior management is committed to ensuring that recommendations arising from such reviews are implemented in a timely fashion.

In addition, the Office seeks to reduce the risks associated with ICT systems/cyberattack by:

- maintaining clear documentation and audit trails
- ensuring segregation of duties between authorisation, payment and reporting functions and within these functions
- providing cybersecurity training and bi-annual simulated phishing exercises
- rotation of staff and
- supervisory checks and
- documented protocol for dealing with service providers, suppliers and clients in the event of a cyberattack.

6. Internal controls

It is important that all staff are aware that fraud can occur, that controls are in place to protect the Office from fraud and to protect the public funds and resources which are entrusted to staff.

The Office acts to prevent fraud through the implementation of controls, which are designed to identify the risk of fraud and minimise the possibility of those occurrences. Regular reviews of internal controls help provide assurance that the Office's objectives will be met. It is an important feature of this approach to fraud prevention that all staff are aware of the potential for fraud and work to ensure that controls are in place to guard against this possibility and detect it quickly if it does occur.

On an annual basis Deputy Directors complete divisional risk assessments and control questionnaires for their areas of responsibility and confirm whether controls are operating effectively. Where controls are considered by Deputy Directors to be inadequate or found to be non-existent the Deputy Directors are required to indicate the steps that will be taken to address the issues identified. The Office's Risk Management Committee considers the assessments and may adjust the risk register accordingly.

The Secretary and Director of Audit is responsible for ensuring that an independent review of the Office's Internal Financial Controls is carried out, on an annual basis, as part of the Office's governance procedures. Reviews of procedures are also regularly completed as part of management's ongoing monitoring of internal controls.

7. Anti-fraud responsibilities

The Office is committed to high standards of integrity, accuracy, openness and accountability in all processes.

All staff

Every staff member has a responsibility to:

- ensure that public funds/assets that are entrusted to them are safeguarded appropriately
- comply with rules of conduct and behaviour as set by Department of Finance circulars (circular 26/04: The Civil Service Code of Standards and Behaviour and the Ethics in Public Office Act 1995 as amended by the Standards in Public Office Act 2001)
- alert their supervisor/audit manager to fraud or suspected fraud. If the supervisor/audit manager is the suspected perpetrator the matter should be reported to the next official in the chain of command
- assist in any investigation that may arise in respect of fraud or suspected fraud
- liaise and co-operate with An Garda Síochána, where required to do so.

Staff should not confront or interview suspects (this is a specialised area and will have implications in any subsequent legal proceedings) or contact the Garda Síochána as this is a matter for management to initiate.

Line Managers

Line Managers (Auditor/Audit Manager) are expected to set an example by complying fully with procedures and controls.

The day-to-day responsibility for the prevention and detection of fraud rests with line managers who are responsible for:

- Identifying the risks to which systems, operations and procedures are exposed
- Developing and maintaining effective controls to prevent and detect fraud
- Ensuring that controls are being complied with
- Providing induction and regular training for staff involved in internal control systems to ensure that their responsibilities are regularly highlighted and reinforced, and
- Ensuring segregation of duties, supervisory checks and keeping the rotation of staff under review.

Where a member of staff alerts a supervisor/line manager/senior management to a possible fraud, the person to whom the matter is reported must:

- immediately report the matter to the **Secretary and Director of Audit**¹
- preserve any evidence including documentation, ICT logs etc.

Senior Management

It is the responsibility of senior management (Secretary and Director of Audit, Directors and Deputy Directors) to:

- Ensure suitable policies and practices are in place to safeguard the Office against fraud and theft
- Provide specialised training for management/staff who have designated roles
- Ensure that the formal policy statement is communicated to all staff
- Report allegations of fraud and the results of investigations into such allegations, to the internal auditors, external auditors and the Audit Committee
- Carry out vigorous and prompt investigations if fraud occurs or is suspected
- Produce a written report (acknowledged by supervisor/line manager/senior management)
- Take appropriate action to recover any loss
- Report incidences of fraud or suspected fraud to the Gardaí and meet with Gardaí if required
- Take appropriate legal and/or disciplinary action, including under the Civil Service Disciplinary Code (Circular 19/2016) against perpetrators / suspected perpetrators of fraud and
- Take disciplinary action, including under the Civil Service Disciplinary Code (Circular19/2016) or otherwise as appropriate against line managers and supervisors where their failures/lack of due care for State resources has caused or is suspected of causing unacceptable loss or damage to the Office.

In general, it is the responsibility of the Secretary and Director of Audit to communicate with the relevant authorities (e.g. Garda Síochána) in relation to fraud or other forms of wrongdoing.

Finance Unit

The Finance Unit is responsible for:

- the development and implementation of internal financial controls, accounting policies, practices and procedures for the Office and
- monitoring the implementation of these controls, policies, practices and procedures in the Office.

¹ The Secretary and Director of Audit shall, upon receipt of information indicating that a fraud or suspected fraud has occurred, seek the appropriate legal advice, then conduct an investigation complying with the Civil Service Disciplinary Code.

Human Resources, Learning and Development (HR, L&D) Unit

A key measure to deter fraud and corruption is to take effective steps at the recruitment stage to establish, as far as possible, the previous record of potential staff in terms of their propriety and integrity.

The HR, L&D Unit is responsible for:

- communicating rules of conduct on appointment
- ensuring employment policies, including those regarding fraud, acceptable ICT usage and mobile devices usage policies are included in induction programmes for staff at all levels
- providing awareness training to all staff on matters such as the *Office Speak Up policy* and preventing cyberattacks
- monitoring turnover and leave patterns of staff
- providing updates on this to the Secretary and Director of Audit and other relevant employment policies.

Publicjobs is responsible for ensuring that new staff have been vetted (by An Garda Síochána) prior to nomination for appointment. When recruiting under licence or short-term staff (including contractors, students and apprentices), the Office designated 'liaison persons' refer candidates to the National Vetting Bureau (NVB). The NVB makes enquiries to An Garda Síochána or Scheduled Organisations as it deems necessary to establish whether there is any criminal record or specified information relating to the person.

Internal Audit

Internal audit provides reasonable assurance to management that the Office's significant risks are being appropriately managed with an emphasis on internal controls and governance processes. The Office's internal audit services are provided by an external contractor. The responsibilities of the internal auditor are to:

- Review internal controls on areas selected for review
- Provide clear recommendations if control weaknesses are identified
- Ensure audit work takes account of the possibility of fraud.

Internal audit takes a risk based approach when designing the audit programme for the Office which accounts for the possibility of fraud.

ICT Unit

The ICT manager is responsible for ensuring proper controls are in place to reduce the risk of ICT fraud (see also '(v) ICT systems/cyberattack' in section 5 – 'Fraud risk areas').

8. Penalties

It is the Office's policy to prosecute cases of fraud. Any person found guilty of fraud by the Courts, may be fined or receive a prison sentence or both.

In addition, the Office will also pursue other penalties, for example:

- appropriate disciplinary procedures, including dismissal if appropriate
- when the culprit is an individual or company providing services to the Office then contracts for work may be terminated
- the Office will seek full recovery of any money and/or goods defrauded.

9. Reporting fraud

Under the Civil Service Code of Standards and Behaviour civil servants must:

- Maintain high standards in the delivery of services by:
 - being impartial, honest and conscientious in the performance of their duties
 - always acting within the law, and
 - performing their duties efficiently, diligently and with courtesy.
- Observe appropriate behaviour at work by:
 - dealing with the public (for the purposes of the Office this includes any dealings with audited bodies or other State bodies or organisations) sympathetically, fairly and promptly, and
 - treating their colleagues with respect.
- Maintain the highest standards of probity by:
 - conducting themselves with honesty, impartiality and integrity
 - avoiding conflicts of interest
 - abiding by guidelines in respect of offers of gifts or hospitality, and
 - never seeking to use improper influence to affect decisions concerning their official positions.

Under the Office [Speak Up policy](#), all staff have a responsibility to **Speak Up** if they suspect or believe actual wrongdoing has occurred or is occurring including fraud.

The *Speak Up policy* provides information on how staff can **Speak Up** in confidence and in the knowledge that their concerns will be investigated thoroughly, fairly and without reprisal. It includes information on who they should talk to if they have concerns and how to make a formal disclosure report. It also outlines the steps that will be taken by the Office following receipt of a disclosure, the protections available under the protected disclosures legislation and the remedies available where the person feels they are being penalised for having made a disclosure.

Reporting procedures (general)

- The procedures for staff reporting concerns in relation to fraud are those set out in the Office *Speak Up* policy for staff.
- In general, if any staff member (the reportee) has concerns regarding fraud, then he or she should normally raise those concerns initially with their line management or the Deputy Director for Central Services.
- If the reportee is reluctant to do so for any reason or wishes to formally report a concern, then he or she should follow the steps below:
 - email speakup@audit.gov.ie (this address is only accessible by the Secretary and Director of Audit and the Deputy Director for Central Services), or
 - speak to, email or write to the Deputy Director for Central Services or the Secretary and Director of Audit.
- All reported matters will be logged and an initial assessment conducted to establish if there is prima facie evidence that a wrongdoing has occurred and if an investigation is warranted.
- Where an investigation is required, the investigation will be undertaken by an appropriate senior member of staff or by a third party appointed by the Office.
- This investigation will include a determination of any action necessary to address the issue of concern.
- The reportee will be updated on the progress and outcome of the investigation as appropriate, having regard to the nature of the matters investigated.
- All investigations of fraud will be reported to the Chairperson of the Office's Audit Committee and the Audit Board as appropriate. It should be noted that it may not be possible to inform the staff member reporting the violation, or suspected violation, of the precise action to be taken, where this would infringe a duty of confidence owed to someone else. The process will be as open as possible subject to these constraints. Any matter reported under this policy will be promptly investigated, with due regard to the dignity of all concerned, and appropriate corrective action or disciplinary action, in line with the Office's disciplinary procedures, if warranted, will be taken following the investigation. It is not possible to lay down precise timescales or steps required for investigations, as this will depend on the nature of the issue. However, the Office will ensure that the investigators will use all reasonable speed without affecting the quality or depth of the investigation.

- Every effort will be made in accordance with the protected disclosures legislation to protect the identity of any person making a disclosure report. Disclosure reports and details of any associated work or investigations will only ever be shared with a limited number of people on a strict **need-to-know** basis unless for example, the Office has an obligation to disclose the information under law or where it is in the public interest to do so.
- In general, where the Office deems it necessary to disclose the reportee's identity to a third party, the Office will inform the reportee in advance of doing so and explain the reasons why it is considered necessary.

The Office is a member of the Integrity at Work programme, a Transparency International (TI) Ireland initiative that helps foster workplaces where staff are supported to raise concerns of wrongdoing and act with integrity. The Office has signed the Integrity at Work pledge. Free and confidential advice is available from TI Ireland with relevant contact details available to staff on the Office's intranet.

10. Lessons learned

It is important that where an analysis of risk and/or investigation arising from a disclosure or other circumstances indicate that a fraud has occurred or there is a vulnerability identified, then appropriate actions must be taken.

In considering the actions, the responsible Deputy Director should assess any related threats and the necessary actions to improve controls.

Remedial actions and target dates should be identified by the relevant Deputy Director together with the official responsible for their implementation. This should be communicated to both the Management Board and Audit Committee.

The Management Board should specifically consider (i) how to disseminate the lessons learned from the experience and (ii) whether other actions are required (e.g. revisions to Office policies).

11. Policy review and approval

This policy will be reviewed annually by the Management Board and will be amended if required. Where existing policy reviews require only minor changes or updates, then the delegated senior officer of the responsible unit / owner may approve the policy changes.

12. Policy acceptance by staff

All staff must confirm on an annual basis that they have read and understood the reviewed policy which will be made available on the Office intranet and on the Office's external website.