Fraud and Corruption Control Policy and Procedure

Owner	**Governance and Assurance**	**CHD/2018/4310**
Last Reviewed	**30/01/2020**	**Version 1.05**

1. Purpose

This document outlines:

- principles regarding the prevention and detection of, and response to fraud and corruption within the department
- the department's fraud and corruption prevention model
- the process through which fraud and corruption risks are identified and managed
- associated departmental roles and responsibilities.

This document is supported by the Fraud and Corruption Control Plan, which outlines mitigations for fraud and corruption occurrences in relation to inherently high-risk functions.

2. Policy

The department recognises the management of fraud, corruption and misconduct as being fundamental to good governance practices.

The department is committed to:

- demonstrating a zero tolerance stance towards fraud, corruption and misconduct
- transparent, ethical and accountable behaviour
- minimising the risks of fraud, corruption and misconduct associated with its operations
- addressing any incidents of suspected fraud, corruption or misconduct by its employees.

3. Principles

The department makes the following commitments to the creation and maintenance of an ethical workplace.
The department will:

- ensure that conduct throughout the department reflects the public service values
- apply risk management principles and implement appropriate controls and treatments to minimise fraud, corruption and misconduct, establishing clear lines of accountability for identified actions
- ensure effective internal fraud, corruption and misconduct risk assessment, monitoring and reporting mechanisms are implemented and maintained and their availability is communicated to employees
- report on incidents of suspected fraud, corruption or misconduct to the appropriate external entities
- ensure protection from reprisals is given to employees who make a public interest disclosure in accordance with the *Public Interest Disclosure Act 2010*
- ensure those involved in fraud, corruption or other misconduct do not benefit from such activity
- implement and maintain a fraud, corruption and misconduct training and awareness program to ensure staff are aware of their obligations in relation to relevant policies and procedures.

Risk management (including fraud and corruption risk management) is a requirement of the Financial and Performance Management Standard 2019 and the *Financial Accountability Act 2009*.

4. Scope

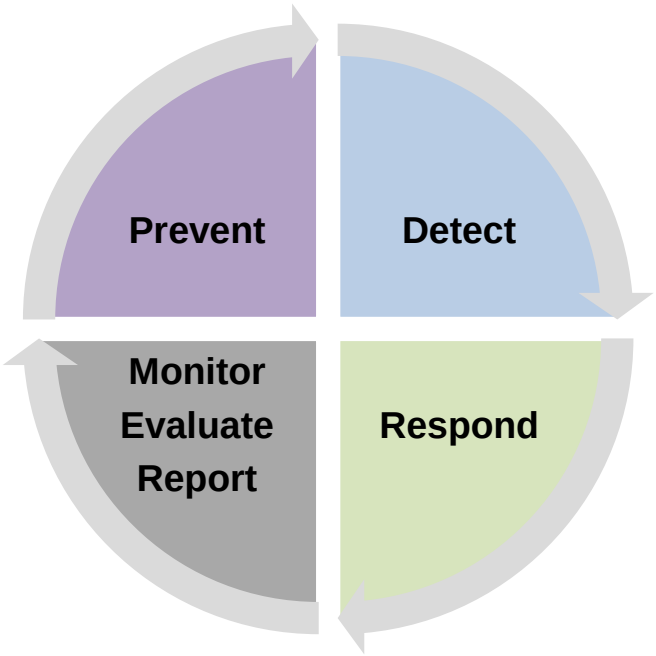
This policy applies to all departmental employees and individuals engaged by the department through other means, as articulated below:

- permanent employees
- temporary employees
- employees seconded from another department
- contractors
- consultants
- volunteers
- trainees
- third-party agents, where applicable.

5. Fraud and Corruption Prevention Model

The department adopts a systematic approach to prevent, detect, respond to, monitor, evaluate and review risks of fraud and corruption.

The diagram below depicts the overarching Fraud and Corruption Prevention Model (the Model). It should be noted that some elements of the Model apply to more than one stage.



5.1 Prevent

5.1.1 Policies and procedures

In addition to this document, the below departmental artefacts support the Fraud and Corruption Prevention Model:

- Fraud and Corruption Prevention and Response Fact Sheet
- Enterprise Risk Management Framework
- Risk Management Policy
- Risk Management Procedure
- Financial Management Practice Manual
- Applying the Code of Conduct Supplement
- Public Interest Disclosure Policy and Procedure
- Managing Employee Complaints Policy
- Contact with Lobbyists Policy and Procedure
- Procurement Policy
- Procurement Authorisations
- Financial Delegations and Authorisations
- Human Resource Delegations
- Conflict of Interest Management Guide
- Conflict of Interest/Declaration of Interests Policy.

It is important to note that whilst the above documents are critical enablers of the Model, the document provisions must be consistently applied in order to be effective. The assumption that controls are being applied is not sufficient for high-risk functions. Periodic spot checks (such as random sampling) must form part of the control framework within business units involved in high-risk functions.

5.1.2 Ethical culture

A strong ethical culture supports the prevention, identification and effective management of fraud, corruption and misconduct. All staff are responsible for contributing to fraud and corruption risk management. The provision of training and implementation of awareness activities helps ensure that employees are aware of this obligation.

Leaders and managers play a key role in modelling ethical behaviour.

The Code of Conduct for the Queensland Public Service, *Public Sector Ethics Act 1994* and *Crime and Corruption Act 2001* provides guidance on the standard of behaviour expected of employees in undertaking their duties with integrity and ethics.

Applying the Code of Conduct Supplement provides more information on how the Code of Conduct works in the department and supports employees in making ethical decisions in their day-to-day work.

5.1.3 Roles and responsibilities

Refer to **Appendix A** for a detailed overview of responsibilities.

5.1.4 Risk assessments and review

All departmental risk management activities are to include fraud and corruption risk identification and assessment.

Fraud and corruption risk assessments must be completed at least every two years by business areas that perform high-risk functions, as defined in the Fraud and Corruption Prevention Control Plan. More frequent assessments may be required, such as due to an escalated risk level or material change to the business environment.

In addition, Governance and Assurance, DITID Corporate, will lead the formal annual review of fraud, corruption and misconduct risks, with input from risk owners and risk treatment officers. On an operational basis, fraud and corruption risks and preventive controls will be monitored, tested and reviewed by the risk owner and escalated as required, in accordance with the Enterprise Risk Management Framework.

When dealing with large investments and/or sensitive negotiations, business areas should consider probity requirements and determine whether the need exists to engage a probity auditor as part of their risk mitigation strategy.

Risk assessments should be tested in conjunction with major change programs to ensure they remain relevant and effective.

5.1.5 Internal controls

Internal controls help to maintain the integrity of systems and processes, safeguard assets and encourage compliance. Continual monitoring and reviewing of the department's internal processes is an embedded component of the normal management process.

Further internal controls may be developed to manage fraud and corruption risks. If high or extreme risks are identified as part of a risk assessment, a fraud and corruption control plan must be developed to ensure the adequate and effective treatment of the risks.

Fraud and corruption controls should be cost-effective, efficient, appropriately documented and subject to ongoing review and refinement. Such controls may include:

- pre-employment screening
- internal transaction checks or post-transaction reviews
- system access controls.

Departmental employees within the scope of this document have the responsibility to adhere to internal controls, including the escalation of control weaknesses where these are identified. Inadequate controls, or the overriding of them, will facilitate fraud and/or corruption.

All managers are responsible for ensuring their employees are applying controls as required.

As for risk assessments, internal controls should be tested in conjunction with major change programs to ensure they remain relevant and effective.

5.2 Detect

5.2.1 Employee awareness and training

DITID Corporate's People and Engagement and Governance and Assurance teams work in partnership to design and implement fraud, corruption and misconduct training and awareness activities, in support of the ongoing maturation of the department's risk management culture.

Employees and individuals engaged by the department through other means (as listed in section 4 of this document) have the obligation to complete mandatory online training modules for Fraud Awareness and Corruption Prevention and the Code of Conduct and Ethical Decision-making.

Managers are responsible for ensuring staff prioritise the completion of the modules within one (1) month of their commencement with the department, to thereafter be re-completed:

- Fraud Awareness and Corruption Prevention – every two (2) years
- Code of Conduct and Ethical Decision-making – every year.

Mandatory face-to-face fraud and corruption awareness sessions are convened as needed – that is, to target a particular employee/business group or fraud risk. Attendance at these sessions must be prioritised by the employee group for whom they have been identified as compulsory.

In addition to managing training activities, DITID Corporate develops ongoing, periodic staff communiques and broadcasts regarding events such as Fraud and Corruption Awareness Week, and to provide insight, resources and preventative lessons from recent investigations and prosecutions.

Leaders and managers should also reinforce fraud and corruption risk awareness through activities such as discussions at team meetings, and business unit-level management and supervisor coaching and mentoring.

Appendix B outlines fraud and corruption red flags for employees' review and awareness, to support ongoing detection of potential fraud and corruption.

5.2.2 Public Interest Disclosure and staff reporting

The department's Public Interest Disclosure Policy and Procedure and Managing Employee Complaints Policy outline how a public interest disclosure (PID) and/or employee complaint is assessed and investigated.

A PID is a disclosure under Chapter 2 of the *Public Interest Disclosure Act 2010* (PIDA), and may exist where the allegations refer to suspected fraud, corruption or maladministration by an employee.

Under the Code of Conduct, employees are required to report wrongdoing. The Public Interest Disclosure Policy and Procedure states that when making a disclosure of wrongdoing, employees are encouraged to do so internally (in writing or verbally) to:

- a manager/supervisor
- any other person in a management role within the department
- a complaints manager
- the PID Coordinator (Manager, People and Engagement, DITID Corporate).

The term whistleblower is often used to refer to an individual who has disclosed a suspected instance of fraud, corruption or misconduct. The Public Interest Disclosure Policy and Procedure outlines the following protections for whistleblowers (or disclosers) in alignment with provisions of the PIDA:

- the discloser's identity will be protected where possible
- when making a PID, the discloser has immunity from:
  - civil liability (for example, for defamation)
  - criminal liability (for example, for breaching statutory confidentiality provisions)
  - disciplinary action, termination of employment, or any other workplace or administrative sanctions.

In particular, sections 5.3.4 and 5.3.5 of the Public Interest Disclosure Policy and Procedure outlines the department's obligations to protect whistleblowers and manage reprisals, while section 5.1.6 outlines the circumstances under which a PID is eligible for protection.

5.2.3 Internal reporting and data analysis

The reporting and management of allegations of fraud, corruption and misconduct by an employee will be in accordance with the department's Public Interest Disclosure Policy and Procedure, and Managing Employee Complaints Policy.

Information on fraud, corruption and misconduct allegations is recorded by People and Engagement, DITID Corporate, and reported to the Audit and Risk Committee (ARC) on a quarterly basis. Reported information includes allegations received, summary of actions, outcomes, recommendations for improvement and value of losses recovered (where applicable).

In addition to being used for reporting purposes, the data is reviewed and analysed for emerging fraud, corruption and misconduct risk trends to aid identification of associated actions/controls (including detections). The collection, storage, security, use and disclosure of the data is managed as per the *Information Privacy Act 2009*.

5.2.4 External reporting

Matters may be reported to an external public sector entity that has the power to investigate or remedy them. Section 5.1.3 of the department's Public Interest Disclosure Policy and Procedure provides a guide that maps the nature of the disclosure with the appropriate external entity to whom the matter should be reported.

Sections 5.1.4 and 5.1.5 of the Public Interest Disclosure Policy and Procedure provides an overview of considerations in relation to disclosures to a Member of Parliament or journalist, respectively.

5.2.5 Internal and external review avenues/appeals

Section 8 of the Public Interest Disclosure Policy and Procedure outlines available internal and external review avenues, including the appeal process.

5.2.6 Community awareness

Community awareness is both a prevention and a detection element of the Fraud and Corruption Prevention Model.

The department demonstrates its commitment to ethical behaviour, accountability and transparency through the publication of the following on the departmental website:

- general information about PIDs
- the Complaints Management Policy
- information about how to lodge a Right to Information request.

5.2.7 Audits

Managers are responsible for monitoring the effectiveness of controls within their business areas and must undertake regular reviews of high-risk functions (for example, through conducting regular spot checks of controls).

Internal Audit Services (IAS) also regularly reviews the effectiveness of internal controls and reports findings to the ARC.

5.3 Respond

5.3.1 Investigations

Allegations of suspected fraud or corruption will be assessed by People and Engagement, DITID Corporate. If an allegation is found to meet the definition of corrupt conduct, as defined in section 15 of the *Crime and Corruption Act 2001*, it will be referred to the Crime and Corruption Commission (CCC).

Matters that fall below the threshold of corrupt conduct will be managed and investigated by People and Engagement. People and Engagement will advise the Chief Finance Officer and Head of Internal Audit of any alleged fraud that would result/has resulted in financial loss. When the investigation is complete, management must ensure the implementation of approved recommendations.

Allegations of fraud committed by a party external to the department will be managed by the business unit subject to the fraud. The business unit will be responsible for determining whether there is sufficient evidence to suggest fraudulent conduct. If necessary, the business unit may need to engage an external party to assist, such as a forensic accountant.

5.3.2 Loss recovery

Fraud and corruption-related losses are managed within the parameters of the relevant policies (being, 2.17 Debt management and 2.24 Losses and write-offs) of the Financial Management Practice Manual. Cost centre managers must take action to deal with the loss and minimise risk of further losses.

5.3.3 Disciplinary action

Where a fraud and/or allegation is substantiated, disciplinary action will be determined in accordance with section 5.3.1 of the Public Interest Disclosure Policy and Procedure.

Appropriate action will be based on the seriousness of the allegations and any CCC recommendations, and may include dismissal or a criminal charge.

5.3.4 Business area remediation actions

Following a fraud or corruption allegation, managers are required to review and improve controls as necessary, update procedures and processes, and ensure all business area employees are aware of any process or procedural

changes. Recommended changes included in the investigation report must also be adopted. The ARC will be informed of proposed actions as required.

5.4 Monitor, evaluate and report

5.4.1 Internal controls assessment

Managers are required to assess the effectiveness of controls within their business areas as part of the risk assessment process, as a key component of the business planning cycle. Periodic spot checks of controls must be undertaken by all managers responsible for high-risk functions. Refer to the Fraud and Corruption Control Plan for further information regarding the department's identified high-risk functions.

5.4.2 Audit and Risk Committee

The ARC provides independent assurance to the Director-General regarding the effectiveness and maturity of the department's risk management framework and activities, which includes fraud and corruption risk management. ARC members assess effectiveness of related policies, procedures and processes, and make recommendations for changes if required. DITID Corporate provides regular reports to the committee on ethics and integrity-related matters.

5.4.3 Internal Audit

IAS undertakes the independent examination and evaluation of departmental governance activities. This includes regular reviews of internal control systems to assess whether the systems provide reasonable risk assurance.

5.4.4 External Audit

The Queensland Audit Office (QAO) undertakes regular independent audit reviews of agencies' risk management processes and controls in order to enhance public sector accountability.

5.4.5 Periodic risk assessments

Risk assessments must be undertaken at a minimum of every two years or earlier if warranted by a significant change in risk profile, or the introduction of a high-risk function to the business.

5.4.6 Regular review of policies, procedures and work practices

Policies and procedures are to be reviewed by policy owners at the minimum frequency identified in each document. However, reviews may be brought forward where warranted by significant legislative changes or to meet another requirement (that is, if document deficiencies have been identified).

5.4.7 Identifying fraud and corruption trends

This involves the identification of key factors that influence fraud and corruption risk and refer to related policies to control the incidence and impact of those risks. Individual responsibilities are detailed in **Appendix A**. People and Engagement, DITID Corporate, is responsible for recording, analysing and reporting identified fraud, corruption or corrupt conduct trends to internal and external agencies (such as the CCC or the QAO).

6. Authority

Code of Conduct for the Queensland Public Service 2011
Crime and Corruption Act 2001
Financial Accountability Act 2009
Financial and Performance Management Standard 2019
DITID Financial Management Practice Manual
Public Records Act 2002
Public Service Act 2008
Public Sector Ethics Act 1994
Public Interest Disclosure Act 2010 (formerly Whistleblowers Protection Act 1994)
Right to Information Act 2009
Information Privacy Act 2009.

7. Responsibilities

Responsibilities are outlined in **Appendix A.**

8. Delegations

Delegations are to be exercised in accordance with the Financial Delegations and Authorisations. Please confirm delegate authority levels prior to exercising any powers.

9. Definitions and glossary of terms

Corruption	Dishonest activity in which an officer (engaged by an agency through any and all means) abuses their position of trust, in order to achieve some personal gain or advantage for themselves, or for another person or legal entity, or to cause a disadvantage to others.
Corrupt conduct	Relating to the performance of a person's duties which: 1. is dishonest or lacks impartiality 2. involves a breach of the trust placed in an officer by virtue of their position 3. is a misuse of officially obtained information. The conduct must be a criminal offence or serious enough to justify dismissal.
Department	The Department of Innovation and Tourism Industry Development.
Fraud	Dishonest activity causing actual or potential financial loss to any person or agency, including theft of moneys or other property by employees or persons external to the agency. Often, deception is used either at the time, immediately before or immediately following the activity. Fraud 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 to dishonestly obtain a benefit for themselves or others.
Internal control	An existing process, policy, procedure, system, device, task or other action that is used to modify the likelihood or the consequence of the risk event occurring.
Maladministration	Action which: • was taken contrary to law • was unreasonable, unjust, oppressive, or improperly discriminatory • was in accordance with a rule of law or a provision of an act or a practice that is or may be unreasonable, unjust, oppressive, or improperly discriminatory in the particular circumstances • for an improper purpose • on irrelevant grounds • having regard to irrelevant considerations • was an action for which reasons should have been given, but were not given • was based wholly or partly on a mistake of law or fact • was wrong.
Misconduct	Conduct, for the purpose of this policy, that is other than fraud and corruption, which breaches laws, policies or the Code of Conduct.
Public Interest Disclosure	A report or complaint about a reasonable suspicion of serious wrongdoing in the public sector, which can be made by an employee or member of the public. The disclosure is made under Chapter 2 of the PIDA and includes all information and help given by the discloser to a proper authority for the disclosure.
Reprisal	Causing, attempting or conspiring to cause detriment to any person because, or in the belief, anybody has made, or may make, a PID or because the other person or someone else is, has been or intends to be involved in a proceeding under the PIDA.
Whistleblower	Also known as disclosers. Individuals who have disclosed a suspected instance of fraud, corruption or misconduct.

10. Related documents

This policy should be read in conjunction with the Fraud and Corruption Control Plan, Enterprise Risk Management Framework, Risk Management Policy and Risk Management Procedure.

11. Information security

Fraud and corruption risk information will be recorded as below:

- **By divisions and programs/projects:** Divisional and program/project risk registers, with advice of all fraud and corruption risks to be escalated to Governance and Assurance, DITID Corporate
- **By Governance and Assurance, DITID Corporate:** whole-of-department fraud risk register.

Information and data about ethics and integrity investigations will be recorded by People and Engagement, DITID Corporate.

Public sector organisations have a duty under the *Public Records Act 2002* to make, keep, manage and dispose of public records (see CCC, Queensland State Archives or the Queensland Ombudsman websites for further information).

12. Further information

For support, advice and assistance employees should contact:

- their manager or supervisor
- the PID Coordinator via email to ethics@ditid.qld.gov.au
- Employee Assistance Program – a free confidential counselling service available on 1800 604 640.

13. Review

The document shall be reviewed within two years of the last reviewed date, or sooner where warranted by significant legislative or other changes.

The review will be led by DITID Corporate to ensure the document's continuing alignment with current whole-of-government fraud and corruption management provisions and best practice, and the departmental and portfolio environment. Where material changes are made, the new version of the document will be consulted with divisions, and approved by the Director-General.

14. Approval

Signed

Damien Walker

Director-General

Department of Innovation and Tourism Industry Development

Date: 17/02/2020

15. Version history

Date	Version	Action	Description / comments
25/07/18	1.00	Endorsed	Corporate identify update to DITID
18/09/18	1.01	Endorsed	Updated links within the policy document
10/04/2019	1.02	Updated	Minor update to document title and hyperlinks
13/11/2019	1.03	Updated	Minor updates to template following department name change
16/12/2019	1.04	Updated	Revision to a combined policy and procedure document, and to include Internal Audit Services' recommended changes
30/01/2020	1.05	Updated	Revised to include feedback obtained during internal stakeholder consultation

16. Keywords

CHD/2018/4310; fraud; corruption; misconduct; public interest disclosure; ethics; integrity; prevention; risks; red flags

Appendix A – Roles and responsibilities

Accountable Officer (the Director-General) is responsible for:

- ensuring public resources are used effectively, efficiently, economically and appropriately in the management of the department (*Public Service Act 2008*)
- creating an ethical workplace culture where employees report suspected wrongdoing and are supported in doing so (*Public Sector Ethics Act 1994*)
- ensuring department policies and procedures provide adequate safeguards for the prevention of fraud (*Financial Accountability Act 2009*)
- ensuring all matters involving suspected corrupt conduct are referred to the CCC (*Crime and Corruption Act 2001*)
- approving changes to this policy to ensure it remains relevant and current.

Executive Management Group (EMG) has collective responsibility to:

- consider recommendations from the ARC in accordance with the committee's charter
- consider and provide a range of treatment options for extreme and high-level risks escalated from business units
- oversee the implementation of approved recommendations arising from reports investigating fraud and corruption allegations
- lead by example to create an ethical workplace culture.

Audit and Risk Committee has responsibility to:

- diligently exercise its terms of reference, duties and responsibilities to support the Director-General in the effective discharge of legislative accountabilities concerning fraud and corruption risk management
- review and provide independent advice and assurance to the Director-General regarding the department's Enterprise Risk and Fraud and Corruption Management frameworks, procedures and work practices
- provide independent assurance to the Director-General regarding external fraud, corruption and misconduct accountability and reporting requirements.

Internal Audit Services has responsibility to:

- plan and lead audits to assess effectiveness of the department's fraud, corruption and misconduct framework and controls, to assess whether systems provide reasonable assurance.

Executive leaders (Deputy Directors-General and equivalent roles) have responsibility to:

- ensure processes are in place to identify, assess and report on fraud and corruption risks within their business areas, that employees are aware of these processes and support is provided to employees who report suspected wrongdoing
- contribute to the development, implementation and monitoring of the DITID Fraud and Corruption Control Plan where necessary
- periodically review the appropriateness of security measures and personnel clearances in place within their business areas with regard to fraud and corruption prevention and detection
- ensure employees complete and/or attend mandatory Fraud and Corruption Control Awareness, Code of Conduct and Ethical Decision-Making training
- ensure employees are aware of and adhering to human resource and financial delegations and relevant DITID policies and procedures
- implement approved recommendations arising from post-investigation reports regarding fraud and corruption allegations
- monitor high-risk function controls vigilantly and reviewing controls when necessary
- direct and oversee the completion of regular spot checks that procedures and processes are being adhered to consistently and accurately.

Chief Finance Officer has responsibility to:

- develop, implement and maintain finance policies, procedures and/or processes
- monitor the efficiency and effectiveness of DITID finance systems and implement corrective action where necessary
- report and advise on strategic finance matters to the Director-General and EMG
- develop, implement and maintain a gifts and benefits register
- report and advise on strategic finance matters to the Director-General and EMG
- develop and maintain Financial Delegations of Authority

- prepare and submit a report signed by the Director-General to the Auditor-General regarding any loss caused by a suspected offence under the Financial and Performance Management Standard 2009, *Criminal Code Act 1899* or any other Act or law
- arrange training and awareness in finance for relevant employees
- ensure action is taken in relation to losses in accordance with departmental financial procedures and delegations for losses and write-offs for losses through fraud and corruption
- participate in investigations and provide input to reports of suspected fraud or corruption, where necessary.

Chief Counsel, In-house Legal, has responsibility to:

- investigate the feasibility of pursuing available avenues to recover losses and ensure those involved in fraud or corruption do not benefit from such activity, upon receiving instructions from the relevant business unit.

Head of Internal Audit has responsibility to:

- participate in investigations into reports of suspected fraud or corruption where necessary
- provide advice on fraud prevention and investigating any suspected fraud matters if requested by the Director-General
- advise the relevant EMG member, Chief Finance Officer and Director, People and Engagement of any suspected fraud or corruption identified as part of an internal audit.

Executive Director, Information Technology Partners, has responsibility to:

- participate in investigations into reports of suspected fraud or corruption where necessary
- develop, implement and maintain Information Communication Technology (ICT) security policies, procedures and work practices
- monitor ICT security
- report and advise on ICT security matters to the Director-General and EMG
- arrange training and awareness in ICT security matters for authorised users.

Director, People and Engagement, DITID Corporate, has responsibility to:

- promote awareness of integrity and accountability issues to employees, managers and supervisors
- ensure Code of Conduct, ethics and misconduct training is developed and made available to all employees to whom this policy and procedure applies
- work in partnership with the Director, Governance and Assurance, to ensure fraud and corruption control awareness training is developed and made available to all employees to whom this policy and procedure applies
- work in partnership with the Director, Governance and Assurance, to lead the development of implementation of a fraud, corruption and misconduct communication, awareness and training program
- direct and oversee the investigation and management of fraud, corruption and misconduct allegations
- report fraud or corruption which is a suspected offence under the *Criminal Code Act 1899* or any other Act or law to the Queensland Police Service, where not already reported by the relevant line manager
- provide direction and support to business areas to ensure sufficient pre-employment checks (that is, referee reports, criminal history and solvency checks) are undertaken for new starters, especially those engaged to work in high-risk functions (such as grants management and procurement)
- develop, implement and maintain policies, procedures and/or processes for:
  - investigation and discipline
  - conflict of interest
  - separation
  - employee complaints (grievances)
  - performance management
  - outside (secondary) employment
  - employment as a lobbyist in the previous two years
- develop and maintain Human Resource Management Delegations of Authority.

Director, Governance and Assurance, DITID Corporate, has responsibility to:

- promote awareness of integrity and accountability issues to employees, managers and supervisors
- ensure fraud and corruption awareness training is developed and made available to all employees to whom this policy and procedure applies
- work in partnership with the Director, People and Engagement, to ensure fraud and corruption control awareness training is developed and made available to all employees to whom this policy and procedure applies

- work in partnership with the Director, People and Engagement, to lead the development of implementation of a fraud, corruption and misconduct communication, awareness and training program
- develop, implement and maintain the departmental Lobbyist Register and Lobbyists Contact Register policy and procedure
- direct and oversee the maintenance of the Enterprise Risk Management and Fraud and Corruption Control Frameworks
- direct and oversee the maintenance of strategic, fraud and corruption risks information on the department's Strategic and Fraud Risk Registers
- monitor effectiveness of the fraud and corruption framework and direct its improvement, including the implementation of review or audit recommendations.

Manager, People and Engagement, DITID Corporate, has responsibility to:

- act as a central referral and coordination point regarding fraud and corruption allegations for employees, investigators and external authorities
- act as the CCC Liaison Officer for the department, assessing allegations of corrupt conduct on behalf of the department and making referrals to the CCC where warranted
- report PIDs to the Public Service Commission
- provide advice and support to the EMG, managers and employees on issues relating to fraud, corruption and misconduct allegations and investigations within the department
- ensure allegations of fraudulent or corrupt activity and misconduct by employees are appropriately managed
- collate, analyse and report on trends identified through fraud, corruption and misconduct investigations to ARC and other stakeholders as necessary to inform appropriate actions and improvements
- contribute to quarterly ARC reporting in relation to ethics and misconduct allegations and awareness activities, and twice-yearly corporate training completion data.

Principal Advisor, Governance and Assurance has responsibility to:

- maintain the departmental Enterprise Risk Management and Fraud and Corruption Control Frameworks
- monitor effectiveness of the fraud and corruption framework and direct its improvement, including the implementation of review or audit recommendations
- periodically review operational risk registers to ensure fraud and corruption risk is being identified and managed, and escalated for inclusion on the whole-of-department Fraud Risk Register (as necessary)
- maintain the departmental Strategic and Fraud Risk Registers
- design, implement and coordinate the periodic fraud and corruption risk assessment process, with input from business units
- identify and report on trends identified through the fraud and corruption risk assessment process
- provide advice to business areas to support the development of appropriate treatment strategies for fraud and corruption risks that are outside of risk appetite/target
- contribute to the development and implementation of departmental fraud, corruption and misconduct training and awareness activities
- ensure this document is reviewed as necessary, and consulted through divisions when there are material changes.

Executive Directors, General Managers, Directors, Managers and equivalent roles have responsibilities to:

- coach employees to promote ethical behaviour and actions in the workplace
- create an ethical culture through coaching, mentoring and leading by example
- ensure the efficient and ethical use of resources
- identify and evaluate fraud and other corruption risks within their areas of responsibility
- implement appropriate controls at the local level to mitigate such risk
- monitor that controls are being consistently and accurately applied through spot checks of processes
- implement approved recommendations arising from reports investigating fraud and corruption incidents
- develop and maintain operational risk registers to ensure fraud, corruption and misconduct risk are being appropriately captured and monitored within their service and program areas
- ensure advice of all identified divisional or program/project fraud and corruption risks is provided to the Governance and Assurance Team, DITID Corporate, for consideration from the whole-of-department perspective and addition to the DITID Fraud Risk Register
- ensure employees are adequately trained in relevant whole-of-government and departmental policies and procedures, ethical decision-making, misconduct and fraud and corruption prevention and the Code of Conduct, including the process for making and managing public interest disclosures

- ensure employees declare:
  - conflicts of interest
  - contact with lobbyists
  - secondary employment
  - gifts and benefits
- report suspected fraud, corruption or misconduct to People and Engagement, DITID Corporate, as soon as possible
- ensure the confidentiality and integrity of any fraud, corruption and misconduct investigation
- actively support employees who report instances of suspected fraud, misconduct or corrupt conduct, and ensure processes are in place to guard against reprisal action
- be aware of their obligations with respect to losses and write-offs under clause 2.24 of the Financial Management Practice Manual.

All employees within the scope of this policy have responsibilities to:

- be aware of, and comply with, relevant whole-of-government and departmental policies and procedures, including the Code of Conduct
- practice high standards of personal honesty and ethical conduct
- contribute to fraud and corruption risk identification and assessment activities as necessary
- contribute to the development of improved systems and procedures that will enhance the department's fraud and corruption risk posture
- safeguard and ensure the legitimate use of information
- complete mandatory online fraud and corruption, and Code of Conduct and ethical decision-making training within required timeframes
- attend mandatory face-to-face fraud and corruption, Code of Conduct and ethical decision-making training and awareness sessions to which they are invited
- follow instructions given by supervisors and managers in relation to safekeeping of departmental assets, corporate credit card use and information and communication technology
- ensure the appropriate declaration of:
  - conflicts of interest
  - other (secondary) employment
  - contact with lobbyists
  - gifts and benefits
- be aware of the possibility that fraud, corruption and theft may exist in the workplace and report any concerns to their manager or supervisor or People and Engagement, DITID Corporate, in accordance with the PID Policy and Procedure
- ensure all personal claims regarding fraud, corruption or misconduct allegations are accurate and contain no deliberate omissions or falsifications.

Appendix B – How do I identify a fraud, corruption or misconduct risk? What are some red flags?

- Focus on what opportunities there may be for inappropriate behaviour by employees and clients in your business.
- If in doubt, raise the issue and discuss it with peers and management through the risk management process.
- You know the nature of your business and what you are going through at the moment; do any of the red flags apply to your areas?
- Risk versus a suspected actual fraud – if you suspect actual fraud or corrupt behaviour, refer it to a delegate and/or seek advice from People and Engagement.

Some discussion points for consideration:

- Emerging areas of research – do managers/supervisors understand the potential and appropriate controls or is excessive reliance placed on one employee?
- Regulatory employees in isolated areas – one-on-one contacts, limited independent overview of decisions, where are the checks and balances?
- Changing organisational structures – does everyone know to whom they report? Do all delegates know for whom they are signing and what they are signing? Are exceptions followed up? For example, a person seeking approval from someone other than their usual supervisor.
- How is time-cheating (that is, inaccurate time or leave recording in timesheets) controlled within business units?
- New relationships with new industries – are we working to the same ethical principles and obligations? Is there scope for misunderstandings about what is appropriate (for example, in relation to gifts and benefits, contacts during contractual negotiations, expectations related to intellectual property sharing)?
- Known low-compliance areas – are there areas where you know the views related to proper procedure are seen as unnecessary overheads? Are there areas where any enquiries related to administrative matters are greeted with hostility, bluster, avoidance?
- Information and intellectual assets – how easy is it for information and intellectual assets to go missing or be misused?
- Recruitment – do you see a need for identity checks and detailed reference and experience checks? How is this done in an emergency?

Red flags for fraud and corruption[1]

Organisational

The following are potential red flags indicating corruption, which have been seen in organisations where corruption was subsequently uncovered.

- Over-zealous acquisition strategies (without proper screening and due diligence, avoiding departmental and State Purchasing Policy requirements, with every purchase seen as urgent or exceptional).
- Autocratic management decisions regarding business relationships, such as a refusal to change a major supplier.
- Unexplained shifts in expenditure patterns.
- Artificial barriers put up to avoid answering questions.
- Excessive secrecy.
- Rumours and low morale.
- A complacent program/project leader/manager.
- Overriding of budgetary controls.
- Discrepancies and deviations.
- Missing records or lack of detail.
- Manual payments or adjustments.
- Consultants given a free reign.

Individual

Red flags in behaviour can either be objective (in that they can be measured or monitored) or subjective (in the sense of being reliant on the managers/ supervisors knowledge of the employee).

Objective red flags are reasonably positive indicators that something is wrong, and can usually be monitored in order to establish the cause of the change in behaviour. Objective red flags can include:

[1] Source – WA Department of Education and Training: Corruption Policy and Control Plan - adapted from SIRCA 01-2003 Fraud Resistance: A Practical Guide

- Signs of excessive wealth or spending, increasing debts and lack of wealth, changes in personal circumstances.
- Long absences from work, poor timekeeping.
- Failure to take leave.
- Changes to work patterns, long hours after normal business hours.
- Manager override of normal controls.
- Excessive use of facilities (that is, telephone, computer or internet) outside normal work areas.
- Obvious unethical or immoral behaviour.
- The finding of a false background.
- Running another business while at work.
- Managers bypassing subordinates.
- Subordinates bypassing managers.
- Review of potential conflicts of interest reveals undeclared personal, business or family relationship with another employee.
- Excessive employee turnover.
- Unexplained employee absences.
- Personal creditors appearing at or contacting workplace.
- Using government facilities while on leave (for example, cab charges, corporate card).

Subjective red flags are more difficult to rely on; they should always be linked to other red flags in the process or systems to which an individual has access.

Subjective red flags include:

- Abnormal social behaviour.
- Problems with gambling, drug or alcohol abuse.
- Excessive mood swings, aggression, marked changes in behaviour.
- Discovered to be a liar, cheat or lawbreaker.
- Overeager to assume other people's duties or to provide help.
- Refusal to relinquish duties.
- Excessive, undeclared use of corporate hospitality.
- Resistance to audit and questions.
- Answering questions and deflecting attention — arrogant and aggressive.
- Providing misleading or ambiguous explanations to questions.
- Gambling (including playing the share market) while at work.
- Borrowing money from fellow employees while at work.
- Secretiveness.
- Refusal, evasion or delay in producing files, minutes or other records.
- Excessive or apparent total lack of ambition.
- Excessive control of records by one officer
- Covering up inefficiencies.

Process

Red flags in a process arise from anomalies on documents or transactions (for example, red flags on payment instructions being processed). Even though accounting and payment employees perform a routine activity with hundreds of transactions per day, they can sometimes spot these anomalies very quickly, including the following:

- Unusual delivery instruction (for example, a purchase order made out to a place other than a department office) with an urgent processing request.
- Photocopied document or attachment.
- Unnecessary words or explanations on the instruction to try and make it seem more plausible.
- Appearance or style not consistent with normal transactions.
- Beneficiary name spelt incorrectly — mismatch with account number, vendor name/number.
- Payment not consistent with the normal business of the vendor or business group.
- Missing expenditure vouchers and unavailable official records.
- Crisis management coupled with a pressured work environment.
- Excessive variations to budgets or contracts.
- Lack of executive or management oversight.
- Reconciliations are not maintained or cannot be balanced.
- Excessive journals.
- Unauthorised changes to systems or work practices.

- Lowest tenders or quotes passed over with minimal or no explanation recorded.
- Lost or missing assets.
- Absence of controls and audit trails.
- Incorrect application of financial and/or human resources delegations.

Technology

Systems-based red flags arise from monitoring routines built into computer and communication systems. They are a powerful means of detecting illicit behaviour. For example:

- Someone logs on to a system using the user identification and password of an employee who is on leave, or attempts to sign on if the password is disabled while the employee is on leave.
- A higher than average number of failed logins.
- Signing on at unusual times of the day.
- Unusual network traffic.
- Controls or audit logs turned off.