

Whitsunday Regional Council

Fraud and Corruption Control Framework

Contents

1. Introduction	3
1.1 Commitment to Fraud Control.....	3
1.2 Major Components of Fraud and Corruption Control Framework.....	3
1.3 Review of the Fraud and Corruption Control Framework	3
1.4 Definitions	3
2. Ethical Culture.....	4
2.1 Understanding Why Fraud is Committed – The Fraud Diamond.....	4
2.2 Embedding an Ethical Culture	5
3. Prevention.....	5
3.1 Internal Controls	5
3.2 Fraud and Corruption Risk Assessment	5
3.3 Pre-Employment Screening	9
3.4 Contractor and Supplier Due Diligence.....	9
4. Detection.....	9
4.1 Reporting Culture of Fraud	9
4.2 Protection For Persons Making a Public Interest Disclosure (formally referred to as a whistle-blower).....	10
4.3 Identification of Early Warning Signs (red flags).....	10
4.4 Data Analysis Program	11
4.5 Post-Incident Review	11
4.6 Procurement Contract Review	11
4.7 Role of Internal Audit.....	11
5. Response, Outcomes and Recovery.....	11
5.1 Assessing and Managing Complaints of Suspected Fraud	11
5.2 Reviewing Systems and Procedures (Post-Fraud).....	12
5.3 Disciplinary Action.....	12
5.4 Recovery of Losses	12

1. Introduction

1.1 Commitment to Fraud Control

WRC has a zero tolerance for corrupt conduct, fraudulent activities or maladministration.

The framework adopted by Council is an integrated approach to the development, implementation and regular review of fraud prevention and detection, monitoring, reporting and response strategies and is based on the Australian Standards Fraud and Corruption Control (AS 8001-2008).

The Director Corporate Services maintains ongoing custodianship of the Policy and Framework.

1.2 Major Components of Fraud and Corruption Control Framework.

The four essential elements of fraud and corruption are contained in Table 1.

Table 1 - Components of Fraud and Corruption Control

1. Ethical Culture	Increasing levels of ethical awareness by embedding and implementing initiatives to deter and minimise the opportunities for fraud.
2. Prevention	Reducing instances of fraud by strengthening the systems of control and risk management.
3. Detection	Implementing initiatives to detect fraud as soon as possible after it occurs.
4. Response, Outcomes and Recovery	Implementing initiatives to deal with detected or suspected fraud in accordance with relevant policies and legislation. Ensuring appropriate outcomes (disciplinary, civil, systemic or criminal justice system), thereby helping to deter and prevent fraud from occurring. Recovery of losses maximised as far as possible, thereby limiting the financial impact and helping to deter and prevent reoccurrence.

1.3 Review of the Fraud and Corruption Control Framework

The framework shall be reviewed at least every two years.

1.4 Definitions

Fraud is a criminal offence as defined in the *Criminal Code Act 1899*.

Fraud is dishonest activity causing actual or potential financial loss to any person or entity including theft of moneys or other property by employees or persons external to the entity and where deception is used at the time, immediately before or 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.

Corruption is a criminal offence as defined in the *Criminal Code Act 1899* and the *Crime and Corruption Act 2001*.

Corruption is dishonest activity in which a Director, executive, manager, employee or contractor of an entity acts contrary to the interests of the entity and abuses his/her position of trust in order to achieve some personal gain or advantage for himself or herself or for another person or entity.

For some examples of fraud and corruption, refer to Table 2 below.

Material loss for an asset belonging to a local government means –

- for money – a loss of more than \$500; or
- for any other asset – a loss valued by the Chief Executive Officer at more than \$1000.

Reportable loss for an asset belonging to the local government, means a loss resulting from:

- the commission of an offence under the Criminal Code or another Act;
- the corrupt conduct of a Councillor, local government employee or local government worker;
- conduct of a contractor of the local government that would be corrupt conduct if the contractor were a Councillor, local government employee or local government worker.

Table 2 – Examples of Fraud

Internal	External	Joint (Collusion)
<ul style="list-style-type: none"> • Theft of inventory, plant and equipment • False claims for travel, petty cash, overtime and expenses • Misuse of corporate credit cards and cab charge • Falsifying invoices for goods or services • Dishonesty using purchase or order forms to gain a personal benefit • Dishonest use of intellectual or confidential property • Falsifying hours on timesheet • Working elsewhere without permission whilst on leave (eg sick leave) • Creating false bank accounts to siphon money • False CV 	<ul style="list-style-type: none"> • Hacking into, or interfering with a computer system • Charging for goods or services that are incomplete or not delivered • Fraudulently inflating invoices 	<ul style="list-style-type: none"> • Certification for goods or services as being delivered when they are not • Unlawful or unauthorised release of information • Knowingly making or using forced or falsified documentation • Collusion with external vendors (eg kickbacks and providing insider information etc).

2. Ethical Culture

2.1 Understanding Why Fraud is Committed – The Fraud Diamond

Fraud is more likely occur when:

- There is an incentive or **pressure** to commit fraud
- Weak controls provide **opportunities** to commit fraud

- A person has the **capability** to recognise the opportunity to commit fraud and takes advantage of it
- The person can **rationalise** committing the fraudulent behaviour.

Promoting the awareness of the above contributing elements can support an ethical culture and assist staff in recognising early warning signs (red flags) of fraudulent activity.

2.2 Embedding an Ethical Culture

The expectations upon all staff are outlined in Council's Code of Conduct. The commitments in the Code of Conduct support the expectations of ratepayers and residents of the Whitsunday region that all activities in Council are conducted efficiently, impartially and with integrity.

To ensure staff have sufficient knowledge to recognise early warning signs of fraudulent activity and that staff are aware of how to report their suspicions, Council provide mandatory ethical awareness training. Ethical awareness training sessions introduce the concept of fraud and assists to embed fraud and corruption control within Council's culture.

Other activities that promote fraud and corruption control within Council's culture are:

- Effective communication and example-setting by management
- Communicating de-identified outcomes of investigations as appropriate in order to deter further incidents of fraud occurring
- Regular discussions of ethical standards or behaviours at team meetings
- Measurement of awareness levels through an ethical culture survey of staff

3. Prevention

Key aspects of preventing fraud include ensuring internal controls are effective to manage potential fraud risks, identify control weaknesses and implement measures to address the weaknesses. It is important that Council's fraud risk assessment is reviewed regularly, at least on an annual basis.

3.1 Internal Controls

Internal controls established within Council include governance/committee structures, reporting pathways, delegations and procedures for monitoring the performance of, and accounting for, Council investment.

Internal controls are developed and maintained through the cooperation of all Departments and work areas, including governance, internal audit and the operational finance unit.

3.2 Fraud and Corruption Risk Assessment

Council has adopted an enterprise risk assessment framework that includes the formal identification, analysis and evaluation of fraud and corruption risks through a structured assessment of risks.

3.2.1 Fraud and corruption risk identification

To be effective in identifying fraud and corruption risks a variety of methods will be used, such as:

- Records of prior losses
- Complaints by staff, clients or stakeholders
- Using knowledge and judgement of work colleagues if they know of how the existing controls could be bypassed ie identifying flaws

- Directly observing workplace activities
- Maintaining contemporary knowledge of risks identified in similar organisations
- Advice and recommendations of other relevant organisations

3.2.2 Correspondence and Information Management

All Council staff must ensure confidential information is securely held and only used for the purpose for which it was collected.

The following represent some examples of fraud and corruption risks:

- A former employee obtaining confidential information and providing to a new employer to aid their dealings with Council
- An employee leaking sensitive information to a member of the public
- An employee using information obtained through the performance of their work for private purposes such as debt collection, intimidation or stalking.

3.2.3 Delegations

Delegations within Council establish who is empowered to make decisions and to take action on behalf of Council.

Council staff may exercise their delegation through actions such as approving expenditure, signing requisitions or purchase orders, approving appointments or leave applications, or signing a contract that commits Council to expenditure.

The following represent some examples of fraud and corruption risks:

- Using delegated authority to make a decision for corrupt purposes
- Act outside their delegation for fraudulent or corrupt purposes which will benefit the employee, relative, or someone with whom they are connected
- Awarding a contract to a contractor without proper due consideration of alternative suitable providers
- A manager who signs off on fraudulent overtime claims

3.2.4 Facilities and public resources

All Council staff are accountable for resources they use or have access to in the course of performing their duties. The poor management and misuse of public resources can undermine the integrity and operational efficiency of Council and thereby not provide the public with value for money.

The following represent some examples of fraud and corruption risks:

- Regularly taking resources, such as office supplies, stationary or equipment home for their own personal use, or to sell for their own personal benefit
- Unauthorised use of a motor vehicles
- Unauthorised negotiating of contracts
- Arranging for the disposal of goods and directing a contractor to make payment directly to them instead of a Council account
- Destroying records to cover their own corrupt activities

- Deliberately over-ordering resources to sue the surplus for personal gain.

3.2.5 Finance

Compliance with Council policies and practices, as well as statutory requirements outlined in the Local Government Act and Regulations, is mandatory for all employees. All staff directing and undertaking financial operations should appraise themselves against Council requirements.

The following represent some examples of fraud and corruption risks:

- Manipulating the financial system to make payments to a non-existent supplier, and indirectly to their own financial account
- Colluding with a supplier to produce an invoice price that is higher than necessary in order to receive a payment or some other benefit from the transaction
- Approving invoices for private expenses or colluding to do so for others
- Submitting a false travel or petty cash claim and receiving a benefit to which they are not entitled
- Using Council resources to purchase goods or services for private use
- Senior management inflating balance sheet values to cover up poor performance or mistakes
- Failing to record purchases properly to misappropriate cash
- Charging personal expenses to a Council corporate credit card
- Falsifying, destroying or damaging receipts and other financial records
- Seeking to allocate a grant outside the terms of the agreement and conditions for personal benefit
- Improperly disclosing personal or banking details to third parties.

3.2.6 Human Resource Management

Council's management of staff is governed by policies and industrial awards.

The following represent some examples of fraud and corruption risks:

- Manipulating recruitment and selection procedures to secure the appointment of a close friend or family member or associate
- Management promoting, engaging or giving an employee advantage over others for personal reasons
- Management unfairly disadvantaging, bullying, intimidating or discriminating against employees for personal reasons
- Management taking detrimental action against employees who report official misconduct or maladministration
- An employee or an applicant for an advertised position falsifying qualifications or employment history or references to enhance their prospects of securing the position
- Management knowingly concealing the corrupt conduct of subordinate employees.

3.2.7 Information Management and Information Technology

Council possesses a range of ICT policies and standards regarding information resources. Compliance with these policies and standards is mandatory for all employees.

Whitsunday Regional Council Fraud and Corruption Control Framework

Council is reliant on information management and information technology systems to perform its operations. It is imperative that information is accurate, complete and uncorrupted and that systems can be easily accessed for its intended use while being protected from any misuse.

The following represent some examples of fraud and corruption risks:

- Electronically creating fraudulent documentation and providing to the public to gain a benefit
- Altering or deleting electronic data to prevent evidence of other wrongdoing from being detected or to aid a third party
- Taking advantage of temporarily inoperative information systems to act in a corrupt way
- Placing malware on Council's systems in an attempt to damage software or information held on the system
- Use another employee's computer and/or log-in
- An IT contractor launches a successful attack on Council's systems
- Gaining access to electronic record without proper authority or approval
- An IT contractor building a "back door" into information technology systems that enable inappropriate secret access to alter or delete Council electronic data and records.

3.2.8 Regulatory Compliance

Council has two main areas of risks associated with regulatory compliance. First, Council is subject to legislation and there may be risks associated with breaching the requirements of legislation. Second, Council acts as a regulator and as such; risks may be present regarding the appropriate or inappropriate use of power.

The following represent some examples of fraud and corruption risks:

- Issuing a license to an individual or business based on factors other than objective assessment criteria
- Deciding or recommending not to pursue prosecution because of a personal relationship with the person or business in breach
- Choosing not to audit a person or business because of a relationship with that person or business.

3.2.9 Procurement

Council staff must comply with the Procurement Policy and Purchasing Guide to ensure that processes and procedures uphold the integrity of procurement decision making.

The following represent some examples of fraud and corruption risks:

- Providing commercial-in-confidence information to a tenderer resulting in them obtaining an unfair advantage over other tenderers in the tender process
- Knowingly making payments on fraudulent procurement related claims
- Colluding with a supplier of goods or services to Council for personal gain
- Splitting an order to avoid obtaining competitive quotes in the tendering process or to circumvent Council's established delegation limits for procurement transactions
- Obtaining kickbacks by organising preferential treatment

- Not declaring an existing relationship or secondary employment with a tenderer and seeking to unfairly influence the decision making process.

3.3 Pre-Employment Screening

Council is committed to maintaining public confidence in the integrity of all staff and such all persons engaged in general Council employment are required to have a criminal history check.

Pre-employment screening is one effective means of preventing fraud and may detect falsified qualifications or identify previous criminal convictions for offences.

Council will undertake the following as a minimum:

- Verification of identity
- Verification of right to work in Australia
- Policy criminal history check
- Reference check
- Verification of formal qualifications

3.4 Contractor and Supplier Due Diligence

Council will perform effective due diligence on contractors and suppliers which may include the following:

- Search on company register
- ABN confirmation
- Verification of personal details of directors
- Director bankruptcy search
- Disqualified Director search
- Search of legal proceedings pending and judgements entered

Council will consider ongoing commercial relationships and reassess a future working relationship if it is found that there is an increased risk of fraud or corruption.

4. Detection

Despite Council best efforts in prevention, fraud and corruption may still occur. It is therefore important that specific strategies are in place to detect fraud as soon as possible.

4.1 Reporting Culture of Fraud

Council's Code of Conduct requires all Council staff who become aware of suspected fraudulent or corrupt conduct to report the matter and must do so immediately.

Staff are required to report through line management in the first instance, who will arrange for the matter to be referred to the Chief Executive Officer. For instances where this is not appropriate, a staff member may report the matter directly to the Chief Executive Officer.

Staff should endeavour to manage information confidentially and, once a report is made, take no further action until advised further by the Chief Executive Officer.

Council will ensure complaints and disclosures are managed impartially and provide support and protection from reprisals to disclosers.

4.2 Protection For Persons Making a Public Interest Disclosure (formally referred to as a whistle-blower)

The *Public Interest Disclosure Act 2010* supports the disclosure of improper conduct or wrongdoing and it has powerful provisions for the protection of people who make a public interest disclosure.

Council encourages and facilitates the disclosure of wrongdoing by:

- Promoting the public interest by facilitating complaints and disclosures of wrongdoing
- Ensuring that complaints and disclosures, including those made anonymously, are properly assessed and dealt with, reviewed, or investigated thoroughly and impartially
- Affording support and protection from reprisals to disclosers
- Ensuring confidentiality in relation to all information relating to the public interest disclosure and the identity of the discloser.

4.3 Identification of Early Warning Signs (red flags)

Identifying and acting on warning signs (red flags) is critical to the early detection of fraud.

There are two types of red flags: behavioural and transactional. Transactional red flags refer to unusual or out of the ordinary exchanges related to common business activities. Behavioural red flags refer to unusual actions, behaviours or traits by a person.

Some examples of red flags are provided in the table below.

Table 3 – Early Warning Signs (Red Flags)

Transactional Red Flags
<ul style="list-style-type: none"> • Transaction occurring at an unusual time (of day, week, month, year or season) • Frequency of the transaction is unusual (too many or few) • Place of transaction is unusual (eg invoice not usually received from a country or region) • Amount of the transaction is unusual (too high, too low, too alike, too different) • Unusual relationships between persons (related parties, perceived strange relationship between parties, management performing administrative functions)
Behavioural Red Flags
<ul style="list-style-type: none"> • Employee lifestyle changes (expensive cars, jewellery, homes, clothes) • Exorbitant/excessive lifestyle, personal circumstances or purchases not matched with income (eg significant gambling addiction may increase the likelihood of committing fraud) • Significant personal debt and credit problems • Creditors or collectors appearing at the workplace • Refusing vacations, sick leave or promotions – may have a fear of detection • Lack of a strong code of personal ethics • A strong desire to beat the system • Criminal history • Persistent and/or unnecessary taking control of records • Insisting on working unusual or non-standard business hours • Avoiding or delaying provision of documentation when requested by auditors

4.4 Data Analysis Program

Data analysis is a process of uncovering patterns and relationships in datasets that appear unrelated and discrepancies which may indicate fraud and irregular behaviour. Using data analytic techniques, trends can be examined and investigated which may be indicative of fraudulent conduct.

The Director Corporate Services is responsible for ensuring that the data analysis program focuses on key risk areas, including key fraud risks.

4.5 Post-Incident Review

Council will ensure an effective review process is completed following a critical incident. The review is to include broader assessment of the issue/s and providing recommendations for improvements to practices.

4.6 Procurement Contract Review

Good contract management can minimise fraud through conducting periodic reviews of contracts with external providers.

The periodic review may include:

- Deliverables
- Performance reviews
- Appropriate documentation and record-keeping
- Ongoing supplier due diligence
- Value for money
- Opportunity/capability for conflict of interest
- Verification of invoices.

4.7 Role of Internal Audit

Internal audit can assist management with the evaluation of internal controls and may be involved in fraud investigations.

5. Response, Outcomes and Recovery

5.1 Assessing and Managing Complaints of Suspected Fraud

Where the Chief Executive Officer is aware of a loss of an asset that the Chief Executive Officer is satisfied is a reportable loss, reasonably suspects there has been a reportable loss of an asset, or is aware of a material loss of an asset, the Chief Executive Officer will respond by:

- Creating a written record of the loss or suspected loss which includes the following details:
 - a description of the asset, including its value;
 - the cause of the loss;
 - the action taken by the local government to deal with the loss, including, for example:
 - action to remedy any weakness in the local government's operations; or
 - action taken to recover the loss;
 - approval for writing off the loss.
- Assessing each matter to determine whether or not it meets the thresholds for official misconduct, public interest disclosures, material loss or reportable loss;

- If the Chief Executive Officer is satisfied that the material loss is also a reportable loss, make the appropriate notifications as soon as practicable, but not more than 6 months after the Chief Executive Officer becomes aware of the loss, to the appropriate entity listed below:
 - The Minister;
 - The Auditor-General;
 - For a loss resulting from the commission of an offence under the Criminal Code or another Act – the Queensland Police Service;
 - For a loss resulting from the corrupt conduct of a Councillor, local government employee or local government worker – the Crime and Corruption Commission.
- If the matter could amount to official misconduct, making appropriate referrals;
- If the matter is assessed as a public interest disclosure, making appropriate referrals;
- Conducting investigations according to the principles of natural justice.

5.2 Reviewing Systems and Procedures (Post-Fraud)

It is important that Council reviews the adequacy of the internal control environment (particularly those controls surrounding the fraud incident) and actively plan and implement improvements where required.

5.3 Disciplinary Action

Action taken in response to allegations of fraud and corruption will be in accordance with relevant legislation, policies and the principles of natural justice.

The management of discipline will consider reasonable management and/or disciplinary action against staff resulting from substantiated allegations of fraud or corruption. Action may include, but is not limited to:

- Reprimand
- Reduction in the level of remuneration
- Transfer or redeployment
- Termination of employment

5.4 Recovery of Losses

Council is committed to quantifying fraud losses and maximising the recovery of losses incurred from fraud and corruption activities and will pursue every possible avenue in doing so, including civil recovery.