Crime and Corruption Commission
QUEENSLAND

Fraud and Corruption Control

Best Practice Guide

March 2018

© The State of Queensland (Crime and Corruption Commission) (CCC) 2018

You must keep intact the copyright notice and attribute the State of Queensland, Crime and Corruption Commission as the source of the publication.

The Queensland Government supports and encourages the dissemination and exchange of its information. The copyright in this publication is licensed under a Creative Commons Attribution (BY) 4.0 Australia licence. To view this licence visit http://creativecommons.org/licenses/by/4.0/.

Under this licence you are free, without having to seek permission from the CCC, to use this publication in accordance with the licence terms. For permissions beyond the scope of this licence contact: mailbox@ccc.qld.gov.au

Disclaimer of Liability

While every effort is made to ensure that accurate information is disseminated through this medium, the Crime and Corruption Commission makes no representation about the content and suitability of this information for any purpose. The information provided is only intended to increase awareness and provide general information on the topic. It does not constitute legal advice. The Crime and Corruption Commission does not accept responsibility for any actions undertaken based on the information contained herein.

ISBN 978-1-876986-86-5

Crime and Corruption Commission

GPO Box 3123, Brisbane QLD 4001

Level 2, North Tower Green Square
515 St Pauls Terrace
Fortitude Valley QLD 4006

Phone: 07 3360 6060
(toll-free outside Brisbane: 1800 061 611)
Fax: 07 3360 6333
Email: mailbox@ccc.qld.gov.au

Note: This publication is accessible through the CCC website <www.ccc.qld.gov.au>.

Foreword

The risk to agencies and entities across all spheres of government from fraud and corruption is as high as ever. The speed with which transactions occur through electronic media and the complexity associated with locating funds once they have been stolen can result in those funds being unrecoverable.

The traditional understanding of an "asset" needs to be redefined as information becomes increasingly attractive as a valuable asset which might also be leaked, stolen or hacked.

Often, the reputational damage sustained by an organisation as a result of fraud or corrupt acts can far outweigh the financial value of those losses and can last for many years afterwards.

Auditors-General from the Commonwealth and states have reported that fraud and corruption prevention is not well understood by senior management, leaving their organisations at risk.

The most effective lines of defence against fraud and corruption are: clearly communicated and understood policies and procedures that give guidance to staff about their role in "fraud-proofing" their organisation; strong and effective internal controls; and staff who are engaged and interested in their work are encouraged to report suspected wrongdoing and feel supported when they do. These things speak to the integrity culture of your organisation and underpin how well prepared your organisation can be to prevent fraud and corruption.

This *Fraud and Corruption Control: Best Practice Guide* combines 10 areas on which agencies should focus their fraud and corruption prevention efforts.

I commend this publication to you to assist in the management and protection of the valuable assets entrusted to you by our community.

Alan MacSporran QC

Chairperson

Acknowledgments

This Guide describes an integrated framework of 10 components considered significant for effective fraud and corruption control. The framework is the outcome of extensive consultation and practical experience of Crime and Corruption Commission (CCC) Prevention staff over many years.

The CCC extends its thanks to those organisations who generously agreed to review this document and to the individuals who gave their time to consider the material and provided valuable constructive comments:

- Queensland Audit Office
- Queensland Ombudsman
- Queensland Treasury.

Contents

How to use this Guide

This Guide is written to help organisations develop their fraud and corruption control framework, with the intention that they will create a tailored program to manage their organisation's risks of fraud and corruption effectively. The Guide presents an integrated approach that includes proactive measures designed to enhance system integrity (prevention measures) and reactive responses (reporting, detecting and investigating activities).

The principles and practices discussed in this Guide should be considered best practice for all organisations in receipt of public funds, and can be applied broadly to all public sector, and many private sector, organisations committed to reducing the risks and incidence of fraud and corruption.

Where an action is mandatory for a Queensland Government public service agency, public sector entity or responsible authority,[1] a reference to the relevant legislation or regulation is included.

Each chapter covers one component of the framework and includes a checklist that can be used to assess the organisation's progress towards best practice in the planning and implementation of that component.

When developing or reviewing an organisational program, it may be best to begin with the checklist and then work through the supporting text to address any identified deficiencies or shortfalls.

1 *Public Sector Ethics Act 1994* definitions, pp. 27–28.

Abbreviations

AS 8001:2008	*Australian Standard for Corporate Governance — Fraud and Corruption Control*
AS/NZS ISO 31000:2009	*Australian and New Zealand Standard for Risk management — Principles and guidelines*
CC Act	*Crime and Corruption Act 2001*
CCC	Crime and Corruption Commission
CEO	chief executive officer
CFO	chief finance officer
CMC	Crime and Misconduct Commission
COSO	Committee of Sponsoring Organizations of the Treadway Commission
FA Act	*Financial Accountability Act 2009*
FMPM	*Financial Management Practice Manual*
FPMS	*Financial and Performance Management Standard 2009*
LG Act	*Local Government Act 2009*
LG Reg	Local Government Regulation 2012
PID	public interest disclosure
PID Act	*Public Interest Disclosure Act 2010*
PS Act	*Public Service Act 2008*
PSC	Public Service Commission
PSE Act	*Public Sector Ethics Act 1994*
QAO	Queensland Audit Office
QO	Queensland Ombudsman
QPS	Queensland Police Service
RTI Act	*Right to Information Act 2009*
WHS Act	*Work Health and Safety Act 2011*

Terminology

Agency	as defined in the schedule to the PSE Act – a department, a TAFE institute or statutory TAFE institute, the administrative office of a court or tribunal, or any other entity that is prescribed under a regulation to be a public service agency.
Department	as defined in the FA Act section 8.
Entity	as defined in the schedule to the PSE Act – the parliamentary service, a local government, a university or agricultural college, an entity established under an Act or State or local government authorisation for a public, State or local government purpose.
Organisation	a generic term to describe any government department, agency, entity, statutory authority, local government or university, and any corporation, cooperative, business or business partnership.
Public officer	a generic term to describe any person employed by the state or local government, including permanent, temporary, general and contracted employees, and senior officers and CEOs. This does not include elected representatives including local government councillors.

Introduction: Frameworks for integrity and control

The topics covered in the Introduction are:

(1) Definitions of fraud and corruption

(2) Integrity in the public sector

(3) Integrity frameworks

(4) Fraud and corruption control frameworks.

Definitions of fraud and corruption

Fraud and corruption can take many forms. Fraud is normally characterised by deliberate deception to facilitate or conceal the misappropriation of assets, tangible or intangible. Corruption involves a breach of trust in the performance of official duties.

This publication does not treat fraud and corruption separately, nor does it give one priority over the other. Similarly, it does not deal with all the possible dimensions of fraud and corruption.

In Queensland, fraudulent and corrupt conduct by public officers may fall within the category of "corrupt conduct" under the *Crime and Corruption Act 2001* (CC Act). Under the CC Act, "corruption" refers to both **police misconduct** and **corrupt conduct** in the Queensland public sector, which includes:

- The Legislative Assembly and the parliamentary service
- The Executive Council
- state government departments
- the Queensland Police Service
- statutory authorities
- government-owned corporations
- universities
- local governments
- courts and prisons.

Corrupt conduct is defined in the CC Act sections 14 to 20 as conduct that:

- involves the exercise of a person's official powers in a way that:
  - is not honest or impartial; or
  - is a breach of the trust placed in the person as a public officer; or
  - involves a misuse of official information or material; and
- if proven, is either a criminal offence or a disciplinary breach providing reasonable grounds for the person's dismissal.

Anyone who tries to corrupt a public sector officer can also be guilty of corrupt conduct if the matter involves a criminal offence.

Examples of corrupt conduct:

- A public officer cheating on travel allowances (because it could be a criminal offence and is dishonest)
- A residential-care officer assaulting a client (because assault is a criminal offence and a breach of trust)

- A purchasing officer of a government department accepting “kickbacks” in the tendering process (because it is a criminal offence and dishonest)
- A public officer looking up the department’s records about a client without a valid work need (because it could result in dismissal and it is a misuse of official information)
- A public officer manipulating a selection panel decision to ensure that a relative gets the job (because the conduct in question could result in the dismissal of the officer concerned and lacks impartiality).

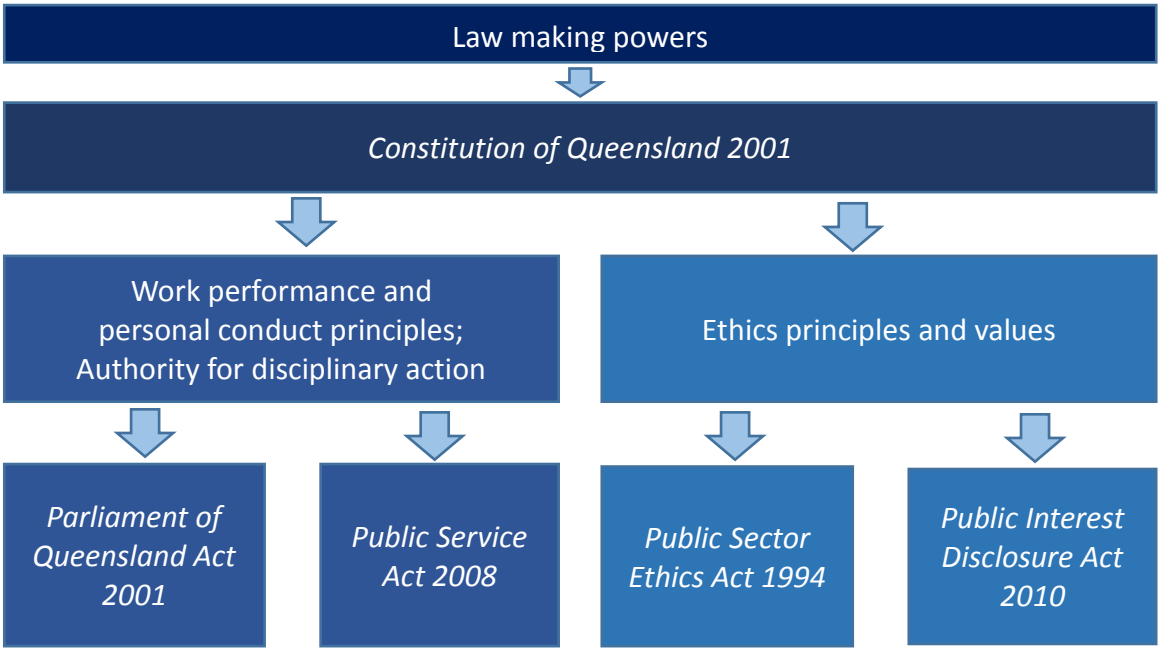
Many forms of fraud and corruption are offences under the *Criminal Code 1899*. These include offences such as extortion, false claims, stealing, issuing false certificates, receipt or solicitation of secret commissions, forgery and election fraud.

Integrity in the public sector

The *Constitution of Queensland 2001* provides the Legislative Assembly with law-making powers. The *Parliament of Queensland Act 2001* and the *Public Service Act 2008* establish work performance and personal conduct principles for serving the government and the public, and authority for disciplinary action. The *Public Sector Ethics Act 1994* and the *Public Interest Disclosure Act 2010* set the ethics principles and values for the public sector.

The following diagram (Figure 1: Ethics legislation) illustrates this legislative ethics framework.

Figure 1: Ethics legislation



Under this framework, public service agencies, public sector entities and public officers are required to seek to promote public confidence in the integrity of the public sector (PSE Act section 6), and public service employees are required to ensure that their conduct meets the highest ethical standards (PSE Act section 6(a)).

Integrity framework

The maintenance of high standards of integrity, conduct and fiduciary responsibility is one of the important tasks of any public sector organisation.

This is managed through a collection of tools (legislation, policies, procedures, etc.), which together determine how the organisation and its staff are to behave on a daily basis and that help the organisation to build an integrity-based culture that will resist fraud and corruption. This is referred to as an integrity framework.

The integrity framework is a risk management tool to protect the organisation from fraud and corruption. It states clear rules and gives sound guidance. Every organisation has an integrity framework, although they might not think of it that way. A good framework can be described as a work in progress because it should always be under review and being modified in order to respond to new threats as they arise. As a consequence, it develops over time through a series of additions, deletions, changes, and continuous improvements.

The integrity framework consists of:

- Legislation – particularly the PSE Act and the PS Act
- strategic plans, mission statements, values etc.
- codes of conduct, policies and procedures
- performance plans
- workplace practices, culture and behaviour, including unwritten ground rules, traditions, etc. (see Chapter 9 for more information)
- the fraud and corruption control framework.

Figure 2: The components of an integrity framework

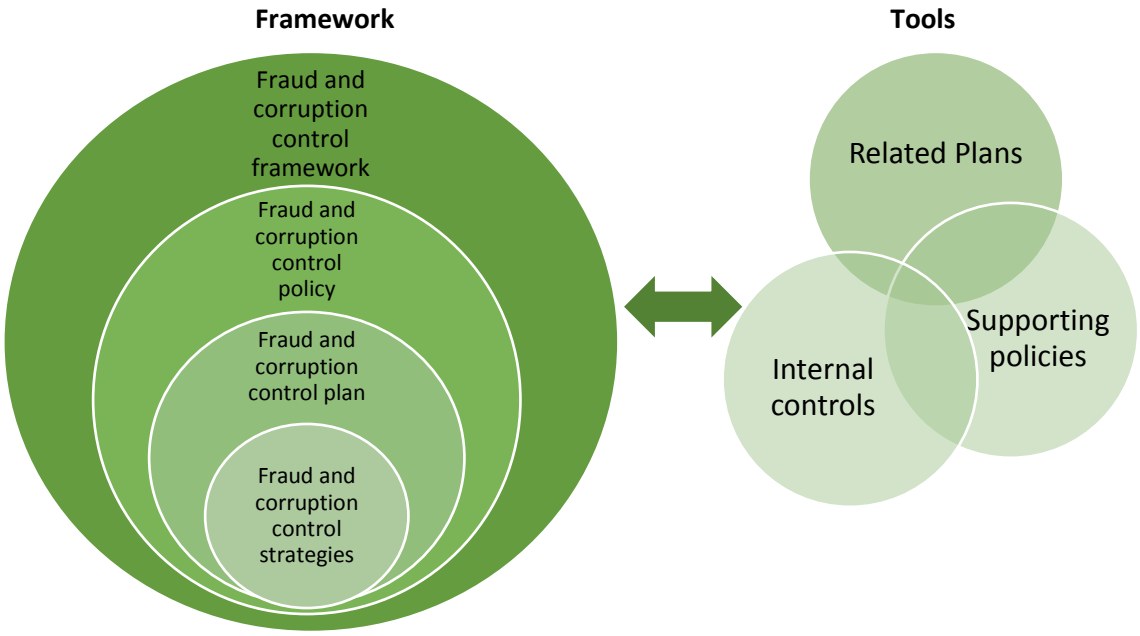
Fraud and corruption control framework

A key component of the integrity framework is the fraud and corruption control framework.

While there is no legislation mandating the implementation of a fraud and corruption control framework, the *Financial Accountability Act 2009* (section 61) and the *Financial and Performance Management Standard 2009* (sections 7, 8 and 28) both require each department's accountable officer and each statutory body to ensure they have a governance framework which includes a risk management system and an internal control structure to mitigate the risk to the department, statutory body and the State from unacceptable costs or losses associated with their operations. One of the significant risk factors for unacceptable costs or losses for any government organisation will be fraud and corruption, and effective mitigation of the risks can only occur through the implementation of a fraud and corruption control framework.

The fraud and corruption control framework consists of coordinated and integrated instruments, mechanisms, arrangements and tools that assist with fraud and corruption control.

Figure 3: Relationship between fraud and corruption control framework components



In order to assist organisations to implement the fraud and corruption control framework, the CCC recommends a best-practice approach through the following 10 components:

(1) Coordination mechanisms
(2) Risk management system
(3) Internal controls
(4) Reporting processes
(5) Protections for disclosers
(6) External reporting
(7) Investigation management processes
(8) Code of conduct
(9) Organisational culture change
(10) Client and community awareness program.

This framework is consistent with the Australian Standards AS8001:2008 for Fraud and Corruption Control and AS/NZS ISO 31000:2009 for Risk Management, and builds on earlier models developed by the CCC.

The 10 components are interrelated. Each one plays an important role, and no one component should be considered in isolation.

Additional readings

- Department of the Premier and Cabinet, Queensland, 2009, Integrity and Accountability in Queensland.
- Department of the Premier and Cabinet, Queensland, 2009, Response to Integrity and Accountability in Queensland.

Chapter 1 – Coordination mechanisms

The topics covered in this chapter are:

- Fraud and corruption control framework coordination
- The fraud and corruption control policy
- The fraud and corruption control plan
- Supporting documents, policies and procedures
- Developing policies, plans and procedures
- Fraud and corruption control oversight
- Communication
- Reviews
- Best-practice targets

Fraud and corruption control framework coordination

Effective mitigation of fraud and corruption risks can only occur through the implementation of a well thought out fraud and corruption control framework designed specifically for your organisation. It is important to ensure that the fraud and corruption control framework is complete and that all components, including those of the integrity framework, work to support each other.

Proper application and management of all components of the framework requires a high level of coordination, for which the primary tools are:

- the fraud and corruption control policy (the Policy), and
- the fraud and corruption control plan (the Plan).

The Policy tells why fraud and corruption control matters, what the organisations aims to achieve and who is responsible.

The Plan details specific actions that are to be taken to achieve the objectives set out in the policy. The Plan should relate to all of the organisation's programs and resources and reflect the organisation's basic corruption prevention policy.

The organisation will also require a range of other policies and procedures to provide details about how it is to perform and manage certain aspects of its work, particularly those activities that have a higher risk of fraud or corruption occurring.

Every organisation needs to have a group of people who have responsibility for monitoring the components of the framework and ensuring the application of the Policy and the implementation of the Plan.

Appropriate oversight will ensure that the Policy, Plan and supporting policies and procedures communicate the organisation's commitment to best practice and create a holistic framework that minimises the risks of fraud and corruption and reinforces organisational integrity.

Ultimately, responsibility for implementing the Policy and the Plan, and deciding who will carry out which specified tasks to achieve the required outcomes is the responsibility of the CEO. While the CEO may delegate some or all of the functions and responsibilities described, the CEO is still answerable to his or her relevant Minister to ensure fraud and corruption is identified and dealt with appropriately.

The fraud and corruption control policy

The purpose of a policy is to provide mandatory directions that regulate the organisation's actions and the conduct of its people. It states how the organisation intends to operate and includes a concise statement of intent and expected outcomes. It should carry the essential information for those who must comply with the policy and its related procedures.

A fraud and corruption control policy should:

- clearly communicate the organisation's values and business practices
- articulate the commitment of the CEO and senior management to these principles
- be based on a risk management approach
- outline its scope and how it will be applied at all levels of the organisation
- identify the key factors that influence fraud and corruption risk
- refer to any relevant legislation
- integrate related and subsidiary policies to control the incidence and impact of risks
- include any necessary tasks, functions, operating parameters and timelines
- state who is covered
- identify any role that has particular responsibilities and accountabilities (e.g. CEO, CFO)
- identify enforcement measures, and
- include version control and review arrangements.

There is no prescribed format for a fraud and corruption control policy. If the organisation already has a template for policies, it can be used.

The Policy should include the following components:

Objectives

Provide a statement of intent and outline why the policy is being written. Explain the intended outcomes of the policy.

Definitions

Define any specific terms or key principles used in the policy to avoid any ambiguity when the policy is applied.

Applicability and responsibility

State who the policy applies to and who will be affected by it, including both internal and external stakeholders. It may also list the people or bodies to whom the policy is relevant and on whom it imposes particular requirements. It may outline individual responsibilities, as well as the links between stakeholders.

Policy statements

Outline what is meant by fraud and corruption and explain its potential impact on the organisation. Provide a clear statement of the organisation's zero-tolerance stance on fraud and corruption, just to remove any doubt.

Procedures

Concisely and briefly outline the control strategies to be used. For example, if you are using the approach in this Guide, you might state that, and list the 10 components:

- fraud and corruption control policy and plan – refer to the organisation's Fraud and Corruption Control Plan as the document that details the specific processes and activities (see section below about the Plan)
- risk management system – explain briefly how the organisation will apply risk management processes to its fraud and corruption control (see Chapter 2)
- internal controls – explain briefly how internal controls will be developed, implemented and reviewed (see Chapter 3)
- reporting processes – state the value placed on reporting by employees and reference the reporting policy and or procedure (see Chapter 4)
- protections for disclosers – be specific about the organisation's commitment to providing protection and support for all disclosers (see Chapter 5)
- external organisational reporting – briefly outline the organisation's obligations to report matters of various types to agencies such as the QAO, the Ombudsman, the CCC and the QPS (see Chapter 6)
- investigation processes – refer to the organisation's Investigations policy and/or procedures (see Chapter 7)
- code of conduct – clearly state the role of the organisation's code of conduct in setting standards for ethical behaviour and the obligations contained in it in relation to fraud and corruption reporting (see Chapter 8)
- organisational culture change – state the organisation's commitment to providing education and training and creating a fraud-resistant culture (see Chapter 9)
- client and community awareness program – state the value placed on creating awareness in the community of the organisation's zero tolerance towards fraud and corruption (see Chapter 10).

Communication

Include a brief explanation of how the policy will be communicated to staff and any other relevant persons or groups.

Legislation, references and authorities

List the relevant legislation, government directives or standards under which the organisation operates that are relevant to the policy, and provide the authority for the fraud and corruption control plan.

Review triggers

List any events that will trigger a review of the policy.

Administrative details/metadata

- the author's name and position
- the approver's name and position
- space for the approver to sign the policy
- space for the date approved
- the date the policy should next be reviewed (at most two years after the approval date).

The fraud and corruption control plan

The fraud and corruption control plan is referred to in the Policy. It contains the details of the organisation's anti-fraud and anti-corruption strategies. The strategies are identified through a thorough risk analysis and assessment process and the Plan states explicitly what actions are to be taken, when by, and who is responsible for them (see Chapter 2 for details on risk analysis and assessment processes.)

The information below provides key features of an effective fraud control plan:

Key features	Comments
An outline of the structure of the organisation.	Include reference to specific fraud control structures in this section of the plan.
A statement of the entity's attitude, definition and approach to fraud.	This statement should match that included in the entity's Fraud Policy and should be endorsed by the Chief Executive.
Demonstrated links to an up-to-date risk assessment.	This promotes the link between fraud risk and fraud control. Examples should be provided to demonstrate this.
Summary of the fraud risks identified.	This promotes awareness among staff of the fraud risks faced by the organisation.
Inclusion of both internal and external fraud risks.	Employees need to be aware of the existence of both internal and external fraud.
Outline of the key controls in place to address all identified high-rated fraud risks.	Information should be provided on the types and nature of fraud controls to inform employees within the organisation. Where possible links should be made to the organisation's business planning process.
A timeline for taking actions on all strategies.	The timeline should include realistic deadlines and monitoring of the implementation of the strategies and controls.
Identification of who has ownership for the design, implementation and evaluation of identified fraud controls.	Assigning ownership is critical in establishing accountability and promoting compliance with the fraud control plan. These responsibilities should also be highlighted in individual performance agreements.
The responsibilities that all employees have for fraud control.	This provides another avenue to remind employees of their responsibilities in relation to fraud control.
Details of how employees can report and respond to suspected fraud.	This should provide employees with information on how, and to whom, they should report suspicion of fraud.
Outline of how fraud is investigated within the organisation.	Information relating to the investigation process enables employees to understand how fraud is investigated and treated within their organisation.
A summary of awareness-raising and training strategies.	This provides information on the fraud awareness-raising activities that are undertaken.
Performance indicators and related targets.	Appropriate performance indicators enable the monitoring of the outcomes of proposed fraud control strategies.

Supporting documents, policies and procedures

Publishing a fraud and corruption control Policy and Plan is a vital step, but the Policy and Plan will only be effective when they are supported by additional appropriately integrated policies and procedures that specify the behaviours required by employees.

Additional documents that are part of the fraud and corruption control framework and that support the Policy and the Plan include:

- the organisation's strategic plan and other management plans (FPMS section 9(1)(a))
- the organisation's operational plan – this identifies the high-level activities that the organisation intends to undertake to assist in the achievement of its objectives, and should include a comment by the Chief Executive on the importance of fraud and corruption prevention (FPMS section 9(1)(b))
- a financial management practice manual (FMPM) for use in the financial management of the organisation – the FMPM is a critical component of the organisation's internal control environment, and consequently it is continually under review and development as other aspects of the internal controls are reviewed and developed (FPMS section 16)
- the organisation's annual budget – the budget should describe the resources that will be applied to fraud and corruption prevention. Program budget goals require managers to be alert to the risk of loss through fraud and corruption. The need for projects to have fraud and corruption controls to ensure that the business receives value for money should be mentioned in the discussion supporting the financial summaries in the budget documents
- the internal audit plan – this should give priority to fraud and corruption prevention through:
  - the internal audit charter, as a basic responsibility
  - specific projects, to support the fraud and corruption prevention activities of managers and other staff
  - all projects, to eliminate the risks identified by control evaluation
- the Code of conduct, including a section dedicated to conflicts of interest
- policies and procedures for:
  - gifts and benefits
  - reporting and managing public interest disclosures
  - investigations
- work procedures and instructions for activities that have inherently high fraud and corruption risks, such as procurement, disposal of assets, and information management.

These supporting documents establish minimum requirements, standards of conduct and controls to enforce the organisation's values, especially in specific corruption risk areas like conflicts of interest or the receipt of gifts and benefits. These additional documents should also be referred to in the Plan.

In addition, the supporting documents that underpin each of the Policy's component elements (e.g. internal controls, investigations, reporting) may in turn rely on their own supporting procedures to explain and give effect to the outcomes required of these policies.

Developing policies, plans and procedures

Fraud and corruption are multi-faceted drivers of dishonest conduct. Therefore, developing good fraud and corruption control policies, plans and procedures requires an in-depth knowledge of an organisation's operations, a clear understanding of the relevant issues, and a good grasp of the ethical principles that underpin the policy objectives in each area.

Developing frameworks for effective fraud and corruption control requires a detailed understanding of the things the organisation does (such as financial and other reporting) and the things the organisation has (assets both tangible and intangible) that others may find valuable.

Dishonest advantage can be gained by people through disingenuous communications designed to mislead or mask the truth. Because of this, the organisation also needs to consider how to prevent fraudulent or corrupt mis-statement of facts or information for dishonest purposes in such things as the Annual Report, financial statements, press releases and other forms of external or internal communications.

A thorough understanding of these issues puts the organisation in the best place to determine the components of the policy, critically analyse where the controls that should protect these assets and processes are weak, and then detail the necessary controls and accountabilities in a plan.

For these reasons, the development of a fraud and corruption control policy and plan and the related procedures is best carried out by a specifically nominated position (E.g. Risk Manager) or a small taskforce with the support of a suitable planning and review committee. The responsible person or group should have suitable experience in risk management and policy formulation as well as practical operational experience.

Because good fraud and corruption policies and plans involve risk management issues, the responsible people should be active members of the organisation's corporate governance or risk management committee, or should have ready access to risk management expertise (either internally or externally).

The impact of the Policy and Plan should be felt at all levels throughout the organisation, so the development person or team must therefore be seen to carry appropriate authority, and will most likely be drawn from the senior management level.

Policy should never be developed in isolation, and employees are critical in the development process. Wide consultation with employees will make it possible to formulate material that not only is suitable for the purpose but also carries grassroots support.

The Policy and Plan should be subjected to searching review by management. Input from key stakeholders should also be sought through a consultative process.

Having these attributes will maximise the opportunities for developing sound, logical policies that are practical and fit for purpose.

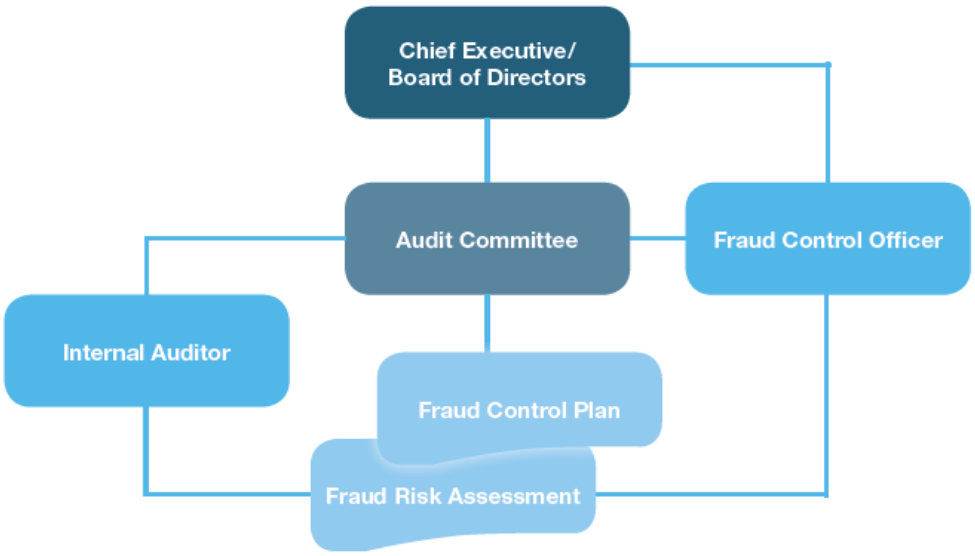
Finally, the Policy and the Plan need to carry the full support of management, and should be universally promoted and accepted, endorsed by any relevant fraud and corruption control committee or coordinator/manager, and approved by the CEO.

Fraud and corruption control oversight

Every organisation will need to ensure that certain management and oversight functions are in place. Key functions are shown in the diagram below. The size of the organisation and the risks it faces will determine the appropriate level of resourcing for each function. In larger organisations these functions might be performed by committees, but in smaller organisations some or all of the functions might be performed by an individual. Regardless of the size of the organisation it is important that management shows its commitment by providing adequate resources for the program and the activities identified in it.

The following diagram gives an overview of key components for oversight of the program.

Figure 4: Fraud and corruption control oversight



Source: KPMG.

Leadership

The Policy and Plan need to be endorsed and supported at the highest level of the organisation, and it is critical that the senior executives are seen to support them in practical ways.

Executive accountability and leadership

The CEO is accountable for fraud control within the organisation and for ensuring that appropriate governance mechanisms and fraud control frameworks are in place and operating as designed.

Corporate Governance oversight

Every organisation needs to have a group of people who have responsibility for monitoring the framework of rules and practices used by the organisation to ensure accountability and transparency in its operations. In the case of a large organisation, this may be a subset of the executive committee or Board of Directors. For smaller organisations it may be the Senior Executive Group (for example, the CEO, CFO, directors, corporate services and HR managers).

As members of this group are likely to have been heavily involved in the development of the Policy and Plan, this is also a useful group to involve in the process of monitoring the implementation and application of the Policy and Plan.

Fraud and corruption control advice

The CEO and executive or board will generally require assistance to fulfil their corporate governance and oversight responsibilities, including: financial reporting, internal control systems, risk management systems, internal and external audit, and fraud and corruption control processes.

This role will include:

- reviewing whether management has in place a current and comprehensive enterprise risk management framework and associated procedures designed to ensure that the identification and management of the organisation's business and financial risks, including fraud, are effective
- reviewing the organisation's fraud control arrangements to satisfy itself the organisation has appropriate processes or systems in place to capture and effectively investigate fraud-related information
- reviewing reports on fraud from the organisation's fraud and corruption control coordinator/manager that outline any identified allegations of fraud, the status of any ongoing investigations, and any changes to identified fraud risk in the organisation
- providing comment on recommendations for change to the internal control structure as a result of liaising with both the internal and external auditors.

This is generally done by an audit committee which would include:

- a Chairperson who is ideally external to the organisation and appointed for periods not less than three years
- the internal auditor
- the head of Corporate Services, and
- (usually) two other staff with recognised and relevant formal or informal qualifications relating to accounting, finance and/or business risk management (ideally not the Risk Management Committee Chairperson).

Treasury Audit Committee Guidelines (Section 3.3) states that it is desirable to have at least two members of the audit committee external to the agency.

The audit committee meetings would also be attended by the external auditor who reports to the committee on the progress of the external audit engagement.

The audit committee has no authority to direct the activities of staff.

In a small organisation the audit committee role might be undertaken by the internal auditor, the corporate services manager, or the finance manager.

The provision of advice by the audit committee or internal auditor does not diminish the responsibility of management or the CEO in the proper execution of their activities.

Risk management oversight

This includes:

- overseeing the development and implementation of a systematic and coordinated risk management framework
- developing a register of risk factors, a risk management plan and controls
- assessing whether the organisation maintains effective risk management practices across all its activities
- ensuring that continuity plans are in place and appropriate, and that the plans are tested and the tests are meaningful

- monitoring the risk environment, and assessing the impact of any changes on the organisation's risk profile
- integrating fraud and corruption matters with the organisation's overall risk profile
- reporting to senior management on risk-related issues
- initiating assessments of how successful the organisation is in embedding an ethical culture.

Normally this will be performed by a committee, comprising:

- a Chairperson who ideally is external to the organisation and appointed for periods not less than three years
- the internal auditor
- the head of Corporate Services
- in-house legal counsel, and
- (usually) two other staff with recognised and relevant formal or informal qualifications relating to business risk management.

In a small organisation this role might be undertaken by a risk management coordinator or Internal Audit.

The Risk Management Committee has no authority to direct the activities of staff. The provision of advice by the Risk Management Committee does not diminish the responsibility of management or the CEO in the proper execution of their activities.

Internal Audit plays a critical role in reviewing an organisation's systems of internal control by using a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes, with particular regard to fraud and corruption. This should include auditing the organisation's fraud risk register to ensure risks are being correctly identified, treated and monitored. The Internal Audit Charter should detail Internal Audit's responsibilities in relation to the management of fraud and corruption risks.

Fraud and corruption control coordination

Clear lines of responsibility and accountability in relation to the coordination, monitoring, review and promotion of the fraud control framework need to be established within an entity to either an individual position or a committee/team appointed for the purpose. This can be achieved through the appointment of a central point of contact for all fraud-related matters. This central point of contact is often referred to as the "fraud manager".

A fraud manager is the individual with delegated responsibility from the CEO/Board for fraud control within an entity. A fraud manager's responsibilities need to be articulated in a fraud control plan and understood by the organisation as a whole. Where such a position is employed, an appropriate line of reporting
is directly to the CEO/Board.

It is critical that the fraud manager has appropriate skills and experience, and be given the authority, time and other resources to discharge this responsibility properly.

Roles would include:

- developing the Policy and Plan and related procedures
- taking ownership of and administering the fraud and corruption control policy
- ensuring that policy changes and procedural recommendations arising from periodic reviews are appropriately prioritised and implemented
- monitoring the performance of staff responsible for implementing the fraud control plan.

A larger organisation, or one with high risk exposure (for example, one that engages with external suppliers for the procurement of goods, services or capital works, or for disbursing grant monies), may also establish a fraud and corruption control committee to deal specifically with fraud and corruption issues.

This committee should have a broad-based (cross-functional) membership to ensure that it can cover at least the areas of highest risk. It should carry a clearly defined responsibility for overseeing the effective implementation of fraud and corruption control measures. This committee has no authority to direct the activities of staff.

Where an organisation is too small to have a fraud and corruption control committee, it may have a fraud and corruption control coordinator or manager instead. This role is usually performed by the CFO, but can also be the Internal Auditor or the head of Corporate Services.

Again, the existence of a fraud and corruption control committee or coordinator does not diminish the responsibility of management or the CEO in the proper execution of their activities.

The following table summarises the functions and accountabilities of key positions.

Function	Position
Accountability for fraud and corruption control Responsibility for ensuring appropriate governance mechanisms and fraud control frameworks are in place and operating as designed.	**CEO**
Leadership Endorsement and support for the fraud and corruption control policy and plan.	**CEO and Executives or Board**
Corporate Governance oversight • Monitoring the implementation and application of the Policy and Plan. • Monitoring the framework of rules and practices used by the organisation to ensure accountability and transparency in its operations.	**Corporate Governance committee** In a large organisation, this may be a sub-set of the Executive Committee or Board of Directors. For smaller organisations it may be the Senior Executive Group (for example, the CEO, CFO, directors, Corporate Services and HR managers)
Risk management oversight Independent and objective review and advice regarding risk management, including: • overseeing the development and implementation of a systematic and coordinated risk management framework • developing a register of risk factors, risk management plan and controls • assessing whether the organisation maintains effective risk management practices across all its activities • ensuring that continuity plans are in place and appropriate, and that the plans are tested and that the tests are meaningful • monitoring the risk environment, and assessing the impact of any changes on the organisation's risk profile • integrating fraud and corruption matters with the organisation's overall risk profile	A large organisation would have a **risk management committee** This committee would include: • a Chairperson who ideally is external to the organisation and appointed for periods not less than three years • the internal auditor • the head of Corporate Services • in-house legal counsel, and • (usually) two other staff with recognised and relevant formal or informal qualifications relating to business risk management. A small organisation might allocate these roles to a **risk management coordinator** or to the internal auditor. A risk management coordinator has no authority to direct the activities of staff.

Function	Position
• reporting to senior management on risk-related issues • assessing whether the organisation is successfully embedding an ethical culture. The provision of advice by the Risk Management Committee does not diminish the responsibility of the CEO in the proper execution of their activities.	
Fraud and corruption control coordination A central point of contact with clear lines of responsibility for all fraud-related matters. Responsibilities include: • developing the fraud and corruption control policy and plan and related procedures • taking ownership of and administering the fraud and corruption control policy • ensuring that policy changes and procedural recommendations arising from periodic reviews are appropriately prioritised and implemented • monitoring the performance of staff responsible for implementing the fraud control plan. The existence of a fraud control manager or committee does not diminish the responsibility of the CEO in the proper execution of their activities.	**Fraud control manager or coordinator** • an individual with delegated responsibility from the CEO/Board for fraud control and reporting directly to the CEO/Board • responsibilities need to be articulated in a Plan and be understood by the whole organisation In a small organisation, this role is usually performed by the CFO, but can also be the Internal Auditor, or the head of Corporate Services. **Larger organisations**, or ones with higher levels of fraud risk, (for example, one that engages with external suppliers for the procurement of goods, services or capital works, or for disbursing grants money) may also establish: • **a fraud and corruption control committee and/or a unit**. It should have a broad-based (cross-functional) membership to ensure that it can cover at least the areas of highest risk, and carry a clearly defined responsibility for overseeing the effective implementation of fraud and corruption control measures. This committee has no authority to direct the activities of staff. • **a fraud control unit** that is responsible for fraud prevention, detection and response activities.
Independent assurance and advice to the CEO/Board regarding fraud and corruption The CEO/Board will generally require assistance to fulfil their corporate governance and oversight responsibilities, including: financial reporting, internal control systems, risk management systems, internal and external audit, and fraud and corruption control. Responsibilities include: • reviewing whether management has in place a current and comprehensive enterprise risk management framework and associated procedures designed to ensure that the identification and management of the organisation's business and financial risks, including fraud, are effective • reviewing the organisation's fraud control arrangements and satisfying itself that the organisation has appropriate processes or systems in place to capture and effectively investigate fraud-related information	**Audit Committee** This committee would include: • a Chairperson who ideally is external to the organisation and appointed for periods not less than three years • the internal auditor • the head of Corporate Services, and • (usually) two other staff with recognised and relevant formal or informal qualifications relating to accounting, finance and/or business risk management (ideally not the Risk Management Committee Chairperson). The Audit Committee meetings would also be attended by the external auditor who reports to the committee on the progress of the external audit engagement. In a small organisation the Audit committee role might be undertaken by the internal auditor, the corporate services manager, or the finance manager. The Audit Committee has no authority to direct the activities of staff.

Function	Position
• reviewing reports that outline any identified allegations of fraud, the status of any ongoing investigations and any changes to identified fraud risk in the organisation • providing comment on recommendations for change to the internal control structure as a result of liaising with both the internal and external auditors.	

Communication

Development of the Policy, Plan and related procedures is only part of the overall process of implementing an effective fraud and corruption control program. Communication of the policy, plan and procedures is critical.

The organisation's officers and other stakeholders are more likely to embrace the underlying ethical principles of a fraud and corruption control policy if they believe that there is a universal commitment to high standards of integrity. The Policy thus needs to be seen to carry the wholehearted endorsement of senior management.

The Plan should be made available to all officers of the organisation. This is usually done by placing the Plan on the organisation's intranet.

The organisation should provide training to develop awareness in employees, stakeholders and the community that fraud and corruption are not acceptable, and that the organisation operates on a zero-tolerance basis.

A communication program designed to suit the various staff levels and job roles, and to cater for regional factors and operational cultures within a single organisation is recommended. The communication activities should send a clear message that responsibility for implementing the policy extends to all levels throughout the organisation.

Ultimately, the goal of policy training and communication is to influence and elevate the organisation's culture by making ethical behaviour the accepted norm. (See Chapter 9.)

The organisation should make its Plan readily available to all stakeholders, including the general public, bearing in mind any confidentiality and security implications. Outlining the measures that have been adopted to prevent and detect both internal and external fraud and corruption should raise the level of awareness of the organisation's business philosophy among suppliers, clients and the community. (See Chapter 10.)

Reviews

The Policy and Plan and each of the subsidiary policies and procedures need to be reviewed regularly to assess performance against predetermined objectives (or targets), and identify any reasons for non-compliance in order to pinpoint any deficiencies and identify improvements. The Australian Standard AS8001:2008 recommends a comprehensive review of the fraud and corruption control plan at least every two years.

Reviews may be appropriate more frequently depending on the organisation's operating environment. An organisation that is affected by rapidly changing legislation, or has to cope with changes in organisational structure (such as following a machinery of government change) and fast-moving technology, may need more frequent reviews than one operating under less turbulent conditions, as these factors may create increased opportunities or incentives to perpetrate and conceal fraud.

Reviews should also be conducted whenever a significant fraud or corruption event or corrupt conduct is detected. Learnings from these may dictate changes in policies and procedures.

The organisation needs to ensure that policy changes and procedural recommendations arising from periodic reviews are appropriately prioritised and implemented. Once again, the best way to ensure that this is done properly is to make their implementation the responsibility of a specific person or group. Progress in implementing the program should be monitored and evaluated through setting targets and using suitable self-evaluation checklists.

Best-practice target

(1) The organisation should have a Policy that clearly states the organisation's zero-tolerance stance on fraud and corruption and provides a holistic control framework.

(2) The Policy should be based on an integrated risk management approach that caters for areas such as internal controls, public interest disclosures, reporting, investigation and training.

(3) The organisation should incorporate the 10 components recommended by the CCC into the Policy and Plan.

(4) The organisation should assign responsibility for development and implementation of the Policy to a nominated senior officer, supported by suitable advisory committees.

(5) The organisation should develop the Policy in consultation with stakeholders and employees at all levels.

(6) The organisation should have a Plan that is supported by the corporate plan, internal audit plan and other management plans, and the annual budget, and has appropriate supporting procedures and operating guidelines in place.

(7) The Policy should be approved by the CEO, and the CEO and senior managers should make their support of the Policy clear to all stakeholders and be seen to be actively implementing the Policy.

(8) The organisation should establish and resource appropriate management and oversight functions, including: Corporate Governance, an audit committee, a risk management committee and a fraud manager.

(9) The organisation should make sure the Policy and Plan can be easily accessed by all internal and external stakeholders and should communicate and promote them throughout the organisation so that all stakeholders and the public are aware of the organisation's commitment to eliminating fraud and corruption.

(10) The organisation should review and evaluate the Policy and Plan frequently to ensure relevance.

Additional readings

- Attorney-General's Department 2017, *Commonwealth fraud control framework 2017*, Australian Government, Canberra <www.ag.gov.au/CrimeAndCorruption/FraudControl/Documents/CommonwealthFraudControlFramework2017.PDF>
- Attorney-General's Department 2017, *Resource Management Guide No. 201 Preventing, detecting and dealing with fraud 2017*, Australian Government, Canberra. <www.ag.gov.au/CrimeAndCorruption/FraudControl/Documents/FraudGuidance.pdf >
- Campbell, Nancy, 1998, *Writing effective policies and procedures: a step-by-step resource for clear communication*, American Management Association, New York.
- Department of Finance Risk resources <www.finance.gov.au/comcover/policy/risk-resources.html>

- New South Wales Audit Office 2015, *Fraud Control Improvement Kit: Managing your Fraud Control Obligations.* <www.audit.nsw.gov.au/ArticleDocuments/197/D1506583%20%20FINAL%20Fraud_Control_Improvement_Kit_February_2015%20whole%20kit.pdf-updated%20August2015.pdf.aspx?Embed=Y>

Checklist: Coordination mechanisms

The following questions are indicative only. Each organisation should develop its own checklist to reflect its specific needs and risk environment. The checklist should be re-examined and updated periodically, as part of the organisation's program of fraud and corruption control appraisal.

- ☐ Does the organisation have a fraud and corruption control policy?
- ☐ Does the policy clearly state the organisation's zero-tolerance stance on fraud and corruption?
- ☐ Is the policy based on a risk-management approach, which identifies and targets those fraud and corruption risks specific to the entity?
- ☐ Does the policy address the following fraud and corruption control elements:
  - ☐ coordination mechanisms
  - ☐ risk management system
  - ☐ internal controls
  - ☐ reporting system
  - ☐ protections and supports for disclosers
  - ☐ organisational reporting
  - ☐ investigation management processes
  - ☐ code of conduct
  - ☐ staff education and organisational culture change program
  - ☐ client and community awareness?
- ☐ Have all relevant stakeholders been involved in developing the overall policy?
- ☐ Does the policy:
  - ☐ clearly communicate the organisation's values and business practices
  - ☐ articulate the commitment of the CEO and senior management to these principles?
- ☐ Is there a person or group designated as owning and administering the fraud and corruption control policy?
- ☐ Does the organisation have a fraud and corruption control plan?
- ☐ Does the plan reflect the organisation's corruption prevention policy?
- ☐ Does the plan include:
  - ☐ mechanisms to identify and record threats
  - ☐ appropriate responses to identified threats
  - ☐ details of the strategies and controls to address identified risks
  - ☐ allocation of responsibility for implementing the strategies
  - ☐ timeframes for implementing the strategies
  - ☐ mechanisms for monitoring the implementation of the strategies?
- ☐ Do the fraud and corruption control plan, corporate plan and other management plans support each other?
- ☐ Does the organisation have other policies and procedures that support the Plan?
- ☐ Do all associated policies and procedures (i.e. associated with fraud and corruption control):
  - ☐ reflect the specific needs of the organisation
  - ☐ complement each other and operate in an integrated and cohesive manner?
- ☐ Has the organisation provided adequate resources for the program?

- ☐ Does the fraud control officer monitor the performance of staff responsible for implementing the fraud control plan?
- ☐ Does the organisation have appropriate management and oversight functions, including:
  - ☐ corporate governance
  - ☐ an audit committee
  - ☐ a risk management committee
  - ☐ a fraud manager?
- ☐ Have the policy and plan been reviewed within the last two years?
- ☐ Are there standing arrangements to review the policy and plan on a periodic basis?
- ☐ Is there a structured approach to implementing significant review recommendations?
- ☐ Have the recommendations for any changes or improvements to policy and operational procedures been prioritised or implemented?
- ☐ Is the policy easily accessible to all stakeholders?
- ☐ Are there effective communication or extension programs to raise awareness of the organisation's fraud and corruption control policy and plan?

Chapter 2 – Risk management system

The topics covered in this chapter are:

- Taking a risk-based approach
- The legislative requirements
- The risk management process
- Recordkeeping
- Oversight of risk management
- Monitoring the process
- Best-practice targets

Taking a risk-based approach

Developing an effective fraud and corruption control program requires a comprehensive understanding of an organisation's risks and vulnerabilities. Identifying an organisation's key fraud and corruption risks is therefore one of the major tasks to be undertaken.

Risk assessment establishes an organisation's risk profile and the nature of the operating environment so that cost-effective practices can be established to contain or minimise each risk. The risk management process provides a logical development framework and methodology from which flow many of the elements of a fraud and corruption control plan — internal controls, reporting systems, the conduct of investigations, and training and awareness activities.

Risk management is good management practice. It is not an "optional extra", to be considered in isolation. It should permeate the organisation's activities and become a normal part of doing business.

The legislative requirements

Risk management is an important element of responsible administration, as set out in the *Financial Accountability Act 2009* (FA Act) and the *Financial and Performance Management Standard 2009* (FPMS).

This legislation requires department's accountable officers and statutory bodies to "adopt a proactive approach in monitoring the appropriateness of systems, operations and overall financial position and performance" of their organisation (FPMS, section 4), and to "establish a governance framework that includes a risk management system" (FPMS, sections 7 and 15).

A risk management system must provide for mitigating the risks to the department or statutory body and the State from unacceptable costs or losses associated with the operations of the department or statutory body, and managing the risks that may affect the ability of the department or statutory body to continue to provide government services. The accountable officer or statutory body may establish a risk management committee, in which case they must have regard to the "Audit committee guidelines – Improving Accountability and Performance", (Queensland Treasury) (FPMS, section 28).

Departmental heads of Internal Audit are responsible for providing advice and assistance with respect to risk management (FA Act, section 78).

The Local Government Regulation 2012 section 164 obligates local governments to keep a written record stating:

(a) the risks the local government's operations are exposed to, and

(b) the control measures adopted to manage the risks.

The risk management process

Risk management consists of the identification and analysis of risk, proceeds to threat assessment and evaluation, and goes through to the final selection of appropriate counter measures.

Australian Standard AS/NZS ISO 31000:2009 recommends a five-step risk management process:

(1) Establish the context

(2) Identify the risks

(3) Analyse the risks

(4) Evaluate the risks, and

(5) Treat the risks.

An alternative risk management methodology is provided in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Fraud Risk Management Guide* (2016) and described in the *Fraud Risk Management Guide: Executive Summary* (2016).

Good communication and extensive consultation with internal and external stakeholders are very important at each stage of the risk management process. The success of the program depends on the extent to which everyone contributes to the assessment of risk and embraces the philosophy of actively managing it. (*AS/NZS ISO 31000:2009*, p.14).

1. Establish the context

> "If you lose money for the firm … I will be very understanding. If you lose reputation for the firm, I will be ruthless." Warren Buffett (to Salomon Brothers employees, 1991)

Different organisations face different fraud and corruption risks, and the first step in risk management is to establish the context of an organisation's risk exposure. *AS/NZS ISO 31000:2009* sets down a number of factors for consideration, which fall into four areas:

- **The external context.** What is the current relationship between the organisation and its environment and interested stakeholders? What are the crucial elements that may affect how the organisation manages the risks it faces?
- **The internal or organisational context.** What are the culture, current goals, objectives, strategies and capabilities of the organisation?
- **The task or activity context.** What are the objectives and strategies of the activity or function to which the risk management process is being applied?
- **The risk criteria.** What criteria are being used to evaluate the significance of the risks?

2. Identify the risks

Unidentified risks cannot be planned for and treated. However, the consequences of "risk types" can be anticipated and planned for. A full understanding of the organisation's exposure to risk will only come from a comprehensive search by all stakeholders for potential risks. The broader the range of stakeholders involved, the more likely it is that all risks will be identified.

The risk analysis must consider not only current threats from internal and external sources but also potential and emerging threats.

Using a variety of techniques helps to identify risks. The search for potential risks may include reviewing the organisation's fraud register and records of prior losses for ongoing risks and trends; analysing process flow charts; interviewing clients and conducting group discussions; analysing audit outcomes; conducting SWOT (Strengths, Weaknesses, Opportunities and Threats) and gap analyses; control risk assessments; scenario analyses; and brainstorming. An inquiring mind is invaluable in identifying potential risks.

Potential risks should not be overlooked or filtered out by premature judgments. The important thing is to adopt a systematic and comprehensive approach so that all potential risks are identified, regardless of their source or controllability.

An organisation may face major challenges in identifying its fraud and corruption risks. In some cases, an organisation's context and the industry environment may highlight particular functions or make some classifications of risk more significant than others.

One starting point is to identify the organisation's major activities, and the nature of the business activities carried out by internal groups on external activities, and the degree to which these internal groups interact with the external entities, such as:

- service outputs and deliverables
- operational areas and functions
- revenue generation and collection activities
- expenditure programs and financial management
- outsourced or contracted operations
- supplier interfaces and other service inputs
- asset utilisation, acquisition and disposal
- client records and support.

Another approach is to build on the work of others and seek out similar bodies that may be willing to share experiences. Consulting firms also often have industry-based and sector-based checklists that can be useful.

Areas of risk to explore

The CMC survey *Profiling the Queensland public sector* (CMC 2004) provides an insight into operational areas and functions perceived to have high levels of fraud and corruption risk, including:

- financial functions – such as the receipt of cash, revenue collection and payment systems, salaries and allowances, entertainment expenses
- construction, development and planning functions – ranging from land rezoning or development applications to construction and building activities
- regulatory functions – involving the inspection, regulation or monitoring of facilities; and operational practices, including the issue of fines or other sanctions
- licensing functions – such as the issue of qualifications or licences to indicate proficiency or enable the performance of certain activities
- demand-driven or allocation-based functions – where demand often exceeds supply, including the allocation of services or grants of public funds, or the provision of subsidies, financial assistance, concessions or other relief
- procurement and purchasing functions – including e-commerce activities, tendering, contract management and administration, and the practices of external agents/contractors/consultants and providers of goods/services
- other functions involving the exercise of discretion, or where there are regular dealings between public sector and private sector personnel (especially operations that are remotely based or have minimal supervision).

3. Analyse the risks

Once the risks have been identified they need to be analysed and assessed to determine their significance so they can be prioritised for treatment.

There is no single template or model for risk assessment. AS 8001:2008 suggests a separate approach for every exercise, but that may not be feasible. The essential requirement is that the method used meets the needs of the organisation — and every organisation is unique.

The most common form of risk analysis is through application of sound judgement or informed decision-making, often known as "qualitative risk analysis". This is done by assessing how likely it is that an event will happen or how frequently it might occur, and determining how serious the potential consequences would be if the event occurred. This process should be undertaken by people within the organisation with sufficient practical experience and a depth of understanding about the organisation and the risks associated with business operations.

Figures 2.1, 2.2 and 2.3 are sample tables for this purpose. Note that each organisation should develop label descriptions to suit its own processes and operating environment.

Figure 2.1: Likelihood scale

Rating	LIKELIHOOD – What is the likelihood of the risk event occurring?
5	**ALMOST CERTAIN:** will probably occur, could occur several times per month
4	**LIKELY:** high probability, likely to arise once per month
3	**POSSIBLE:** reasonable likelihood that it may occur at least once in a year
2	**UNLIKELY:** plausible, could occur over a five-year period
1	**RARE:** very unlikely but not impossible, unlikely over a five-year period

Figure 2.2: Loss or damage impact scale

Rating	IMPACT – What is the potential loss / damage / impact if the event occurs?
5	**EXTREME**: Loss of life, or significant injury. Loss of millions of dollars, major reputational damage
4	**MAJOR**: Organisation's major objectives threatened, or severely affected
3	**MODERATE:** Has some impact on achieving objectives, and requires considerable effort to rectify
2	**MINOR:** Impact on objectives; with some effort, objectives can still be achieved
1	**INSIGNIFICANT:** Very small impact, rectified by normal processes

Combining the assessment of likelihood with the assessment of impact produces a qualitative risk analysis of the seriousness of the risk (Figure 2.3).

This provides a comparative measure for each risk to assist in the evaluation process to guide decision making about the priority of treatment or urgency of action.

Figure 2.3: Qualitative risk analysis matrix

LIKELIHOOD	IMPACT				
	Insignificant	**Minor**	**Moderate**	**Major**	**Extreme**
Almost certain	Medium	Medium	**High**	**Severe**	**Severe**
Likely	Medium	Medium	Medium	**High**	**Severe**
Possible	Low	Medium	Medium	Medium	**High**
Unlikely	Very low	Low	Medium	Medium	Medium
Rare	Very low	Very low	Low	Medium	Medium

4. Evaluate the risks

Risk evaluation involves comparing the level of risk found during the analysis process against the risk criteria established when the context was considered (*AS/NZS ISO 31000:2009*. p. 18).

The evaluation needs to take into account all the factors relevant to the organisation. This is likely to include the impact on the organisation's ability to meet its strategic objectives and continue its operational functions, monetary considerations, the organisation's reputation and employee morale.

The risk evaluation process will help organisations decide on the course of action to take, including:

- whether an activity should be undertaken
- whether a risk needs treatment
- priorities for treatment.

The decisions made should be recorded – a simple risk evaluation worksheet will help with this (Figure 2.4).

Figure 2.4: Risk evaluation worksheet

IDENTIFICATION		ANALYSIS			EVALUATION	TREATMENTS
Area being assessed	**Specific risks**	**Risk degree**			**Current controls or mitigating factors**	**Control improvements**
		Likelihood	**Consequences**	**Risk rating**		

Likelihood	**Consequences**	**Risk rating**
A = Almost certain	1 = Insignificant	S = Severe risk — immediate action required
B = Likely	2 = Minor	H = High risk — senior management attention required
C = Possible	3I = Moderate	M = Medium risk — management responsibility must be specified
D = Unlikely	4 = Major	L = Low risk — manage by routine procedures
E = Rare	5 = Extreme	VL = Very low risk – monitor only

Applying the risk analysis process consistently will identify the risks that need further treatment, and will result in a prioritised list of risks that require consideration in the current period.

5. Treat the risks

The next step is to determine the measures available for treating the risks, assess the treatment options, and prepare, prioritise and implement suitable risk treatment plans (*AS/NZS ISO 31000:2009*, pp. 19–20). Risks are commonly treated using one or more measures that involve:

(1) Accepting the risk

(2) Reducing the likelihood of the risk occurring

(3) Reducing the consequences if the risk occurs

(4) Transferring the risk in full or in part to another party, often contractually or through insurance

(5) Avoiding the risk by deciding not to start or not to continue an activity.

The treatment to be applied to each risk depends on the risk appetite of the organisation and the feasibility and cost-benefit analysis of the available control measures. Every available option should be explored, rather than just adopting the first or most obvious answer.

Risks that fall into the very low, low or acceptable categories may be accepted without further treatment. These risks should be monitored and periodically reviewed to ensure they remain acceptable. Risks in all other categories are to be treated.

Integrity risks require special consideration. It is broadly accepted that a person with integrity will always do the right thing and follow the rules, even when no-one is watching. The challenge for organisations seeking to create a culture of integrity is to set conditions such that people willingly meet those expectations. However, a realistic appraisal of an organisation's integrity risks will include the likelihood that not everyone will consistently act that way. To cater for this, organisations need to set ethical boundaries by means of their policies and procedures. Ultimately, individuals are responsible for exercising their personal integrity through balancing personal interests against the requirements of the organisation and ensuring they make decisions in the public interest. Consequently, organisations should focus on reducing the occurrence of personal integrity failures by reducing the likelihood they will occur. This is achieved by communicating the boundaries and the consequences of failing to adhere to them through regular training, rather than by simply accepting the risk.

The outcome will be a prioritised risk treatment plan that documents the chosen options and how they will be implemented. The plan should include:

- proposed actions
- resource requirements
- responsibilities
- timing
- performance measures
- reporting and monitoring requirements. (*AS/NZS ISO 31000:2009*, p. 20).

Recordkeeping

The process

Every stage of the risk management process involves a wealth of information that can provide:

- a history that allows users to look at previous treatments and how they were implemented to see what worked and what didn't, and so provides an insight into better options
- legal protection – claims of negligence may be defeated or minimised if it can be shown that attempts were made to identify and treat risks
- the means for satisfying external reviews such as independent audits.

To enable this, there should be good quality documentation that includes:

- the results of the appraisal or risk assessment
- the action required as a result of the appraisal or risk assessment
- the reasons and rationale as to why particular treatments were chosen for implementation, including considerations such as cost, ease of implementation and likely effectiveness
- recommendations for follow-up action.

This ensures that the methodology can be replicated to deal with future developments or changes.

Decisions

All decisions made during the risk assessment process should be recorded in a **fraud risk register**, together with the reasons for the decisions (*AS/NZS ISO 31000:2009*, p. 20).

The information below provides guidance regarding the structure of a fraud risk register.

Fraud risk description	The fraud risk is described, ensuring that both the cause and impact of the risk eventuating is covered in the description provided.
Fraud risk factors	These are the conditions or actions which are most likely to cause the risk to eventuate. This is generally a brief list of likely scenarios that could occur.
Inherent likelihood	This provides an indication of how often the risk might eventuate in the absence of any controls. This is generally measured using a five-point scale, e.g. almost certain, likely, possible, unlikely, rare.
Inherent consequence	This provides an indication of how serious the consequences would be if the risk eventuated in the absence of any controls. This is generally measured using a five-point scale, e.g. extreme, major, moderate, minor, insignificant.
Inherent risk rating	This provides a ranking for the risk once the likelihood and consequence of the risk has been considered in the absence of any controls. This is generally measured using a five-point scale, e.g. severe, high, medium, low, very low.
Key controls identified	The key controls are those controls currently established in the entity to minimise the likelihood and consequence of the risk eventuating.
Residual likelihood	This provides an indication of how often the risk might eventuate taking into consideration the effectiveness or otherwise of existing controls. This is generally measured using a five-point scale, e.g. almost certain, likely, possible, unlikely, rare.
Residual consequence	This provides an indication of how serious the consequences would be if the risk eventuated taking into consideration the effectiveness or otherwise of the existing controls. This is generally measured using a five-point scale, e.g. insignificant, minor, moderate, major, extreme.
Residual risk rating	This provides a ranking for the risk once the likelihood and consequence of the risk has been considered taking into consideration the effectiveness or otherwise of the existing controls. This is generally measured using a five-point scale, e.g. severe, high, medium, low, very low.
Fraud risk owner	This is the individual or group within the entity with accountability for managing the identified fraud risk.
Action required	This includes any further actions that the entity must undertake in relation to the identified fraud risk (i.e. new controls to be established).

The Fraud Risk Register is best kept as a separate document from other risk registers as it may also contain sensitive information which not should be more widely accessible than is necessary. This also facilitates monitoring.

Oversight of risk management

Appropriate resourcing and stewardship is needed to make fraud and corruption risk management effective. Clearly designated responsibility for the organisation's fraud and corruption control initiatives will greatly assist communication with all stakeholders, particularly where there is a reporting obligation external to the organisation. It will facilitate developing, implementing, maintaining and reviewing every aspect of the program.

Even if all or part of the risk assessment and policy development tasks are outsourced, overall responsibility for implementing the program should be assigned to a senior officer as part of their normal duties. That person should be a member of any general risk management committee that the organisation sets up. The responsible officer can play an important role in ensuring that the methodology is appropriate, and can help to improve corporate understanding and commitment to the process.

A risk management committee can also be a good source of advice for building an integrated approach to fraud and corruption risk management. The committee can be responsible for:

- overseeing the development of integrated and cost-effective risk management plans
- monitoring the effectiveness of risk management programs
- reporting to senior management on risk-related issues
- integrating fraud and corruption matters with the organisation's overall risk profile
- disseminating information on risk issues throughout the organisation.

Regardless of whether the oversight function is carried out by an individual or a committee, it is critical that the product of this work is captured in the organisation's policies and procedures, which are to be reviewed and updated to address emerging risks.

Given the diversity of risk and its impact on different stakeholders, strong communication programs are needed to guarantee good levels of understanding and consistent operational practices. Education, awareness and communication are discussed in Chapters 9 and 10.

Monitoring the process

Organisational systems and operating environments are constantly changing, and few risks remain static. Consequently, risk identification and assessment (including treatment plans, strategies and control mechanisms) need to be part of a continual review process rather than a one-off event (*AS/NZS ISO 31000:2009*, p. 20).

In addition to continually monitoring the effectiveness of the risk management process, specific events may happen which would trigger a review. Examples of triggers include:

- a fraud or attempted fraud – these will reveal vulnerabilities that had been previously overlooked, or reveal a need for additional controls
- changes in the operating environment – removal of old or implementation of new operating systems and practices can create and/or eliminate risks for an organisation
- identification of emerging risks.

The *Australian Standard AS 8001:2009* recommends a comprehensive review of fraud and corruption risks every two years, depending on circumstances (p. 20). These reviews should consider the organisation's risk exposure in the current environment, threats from both internal and external sources, and emerging risks. The effectiveness of the controls should also be reviewed at this time. This continual process of monitoring and review will ensure that the risk criteria are critically examined and the control mechanisms improved in each review cycle.

Best-practice targets

(1) The organisation should assess fraud and corruption risks using a comprehensive risk management system to establish the level and nature of its exposure to internal and external threats (at least every two years).

(2) The assessment should cover all discrete functions and operations of the organisation.

(3) To ensure an integrated and consistent approach, the fraud and corruption risk assessment should form part of the organisation's overall risk management strategies.

(4) The process of risk evaluation should be based on a comprehensive understanding of the organisation's risk profile within the context of its particular operating environment.

(5) The organisation should allocate sufficient resources to carry out the risk identification and assessment tasks to capture all likely risks and treatment plans to mitigate risks.

(6) The organisation should consider taking out insurance to cover itself against fraudulent losses commensurate with its risk profile, and should review this policy annually.

(7) When dealing with integrity risk, wherever possible, focus on reducing the likelihood by providing adequate training rather than accepting the risk.

(8) The fraud risks and planned actions should be listed and prioritised in a Fraud Risk Register.

(9) The organisation should incorporate the outcomes of risk reviews and control responses into the overall corporate risk strategy to ensure that risk is managed in an integrated manner.

(10) A specific person or group should be made responsible, to ensure effective leadership, coordination and accountability for this process.

Additional readings

- *Australian Standard AS/NZS ISO 31000:2009 – Risk Management – Principles and Guidelines*
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2016 – *Fraud Risk Management Guide*
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2016 – *Fraud Risk Management Guide: Executive Summary*
- Department of Finance, Risk Resources. <www.finance.gov.au/comcover/policy/risk-resources.html>

Checklist: Risk management system

The following questions are indicative only. Each organisation should develop its own checklist to reflect its specific needs and risk environment. The checklist should be re-examined and updated periodically, as part of the organisation's program of fraud and corruption control appraisal.

Legislative requirements

- ☐ Does the organisation have a risk management system? (FAA section 61 (b), FPMS sections 7 and 15(1)(h))
  If yes,
  - ☐ Is it reviewed regularly (at least every two years) to ensure it is still appropriate? (FPMS section 15 (3))
- ☐ If there is a risk management committee, does it have regard to the "Audit committee guidelines – Improving Accountability and Performance", (Queensland Treasury) (FPMS, section 28)?

Recommended Best Practice

- ☐ Does the organisation's risk management system cover fraud and corruption risks?
- ☐ Does the organisation have a comprehensive program of fraud and corruption risk assessment?
- ☐ Does the program of risk assessment use a methodology consistent with the *Australian Standards AS8001: 2008: Fraud and Corruption Control Guidelines* 3.6 and *AS/NZS ISO 31000:2009: Risk Management*?
- ☐ Is the organisation's risk review and assessment process thoroughly documented?
- ☐ If a fraud and corruption risk assessment has been conducted, did it:
  - ☐ actively involve all relevant stakeholders
  - ☐ capture all of the organisation's at-risk functions
  - ☐ establish the vulnerability of business processes and related tasks or activities
  - ☐ identify likely internal and external threats
  - ☐ take account of both current and possible future threats
  - ☐ review data from the organisation's fraud register
  - ☐ rate the probable risks appropriately
  - ☐ consider appropriate controls to both prevent and detect fraud
  - ☐ prioritise the implementation of control treatments accordingly
  - ☐ result in a prioritised treatment plan that documents the chosen options and how they will be implemented
  - ☐ ensure adequate communication
  - ☐ properly store the results to enable accessing this information in the future?
- ☐ Does the organisation have a separate fraud risk register?
  If yes:
  - ☐ Is the Fraud Risk Register reviewed regularly by Internal Audit?
- ☐ Is there a person nominated (or designated committee or taskforce) to be responsible for overseeing the assessment of fraud and corruption risks and any relevant control program?
- ☐ Is there a representative and knowledgeable advisory committee to oversee risk management and provide advice and support to any nominated officer, group, committee or taskforce?
- ☐ Has a comprehensive risk assessment been carried out or has the previous assessment been comprehensively reviewed less than two years ago?

- ☐ If there are indications that reviews of risk exposure in particular areas should be carried out more frequently than every two years, has this been done?
- ☐ If there have been any major changes to the organisation's structure, functions or operating environment in the last two years has a risk review been completed since?
- ☐ Are there mechanisms to generate a risk review in the event of legislation changes?
- ☐ Is there a system for recording and monitoring fraud and corruption incidents?
- ☐ Is there a process to trigger a review in response to a fraud event?
- ☐ Are the fraud or corruption incident records maintained in a fraud or corruption register?
- ☐ Are fraud or corruption incidents analysed (for the purpose of identifying trends and emerging threats) at the time that other organisation risk assessments are carried out?

Chapter 3 – Internal controls

The topics covered in this chapter are:

- The significance of internal controls
- The legislative requirements
- The essentials of internal control
- Responsibility for internal controls
- The limitations of control
- Monitoring effectiveness
- Reporting on controls
- Best-practice targets

The significance of internal controls

Internal controls are considered by many to be the first line of defence in the fight against fraud (*AS 8001:2008*, p.29).

Once an organisation has established its risk profile through a comprehensive risk assessment process, it can establish internal controls to deal with and minimise those risks.

> Internal controls cannot guarantee that there is no error or fraud. They can, however, reduce the risk of error and fraud occurring in the first place, and can help to detect fraud and error where it has occurred. (QAO Report 5, 2012, p. 5)

The legislative requirements

State government

For Queensland government departments and statutory bodies (as defined in the *Financial Accountability Act 2009*), internal controls are mandated in two key pieces of legislation, both of which relate to financial management and accountability:

- *Financial Accountability Act 2009* (FA Act)
- *Finance and Performance Management Standard 2009* (FPMS).

The legislation deals with public sector financial management through a principles-based approach, requiring accountabilities and outcomes, rather than prescribing processes. This is a substance-over-form approach, which provides organisations with the flexibility to manage their operations in the most cost effective manner. It allows organisations to develop and implement systems of internal control which best suit their circumstances while still meeting prescribed accountability requirements.

The requirement to establish an internal control structure is found in the FA Act section 61 and the FPMS section 8.

The prescribed accountabilities in the FPMS section 8 are as follows:

- The internal control structure must have a strong emphasis on accountability, best-practice management of the resources of the organisation and internal controls, and must include:
  - an organisational structure and delegations that are supportive of the objectives and operations of the organisation
  - employment of qualified and competent officers, training of the officers and assessment of their performance
  - procedures for monitoring the performance of, and accounting for its investment in, any other entity controlled by the organisation
  - mechanisms to ensure the efficient, effective and economic operation of any internal audit function, audit committee or risk management committee.
- In establishing the internal control structure, the accountable officer or statutory body (section 65 FA Act) must have regard to the *Financial Accountability Handbook* published by Queensland Treasury.
- The internal control structure must be clearly set out and explained in the financial management practice manual of the organisation.
- To the extent practicable, an accountable officer or statutory body must ensure there is an appropriate separation of duties between officers of their organisation.

In addition, section 29 of the FA Act creates a requirement for accountable officers to establish an internal audit function. Statutory bodies are to establish an internal audit function if their Minister so directs or if the statutory body considers it is appropriate to do so.

Section 15 requires accountable officers and statutory bodies to regularly review key governance and control systems to ensure they remain appropriate for managing the financial resources of the department or statutory body.

Under the FA Act:

- Public Service departments' CFOs are also responsible for the establishment, maintenance and review of financial internal controls, and then reporting on the internal controls in an annual statement to the accountable officer (section 77). (Also the FPMS section 57.)
- Departmental heads of Internal Audit are responsible for providing advice and assistance with respect to internal controls and risk management (section 78).

Local government

For Queensland local government, the key piece of legislation that mandates internal controls is the Local Government Regulation 2012 (LG Reg).

LG Reg section 164 states that a local government must keep a written record stating:

- the risks the local government's operations are exposed to, to the extent they are relevant to financial management, and
- the control measures adopted to manage the risks.

The essentials of internal control

Effective internal control requires an integrated internal control structure. This structure consists of the policies, procedures, processes, tasks and other tangible and intangible factors put in place by an organisation to manage operational, financial, compliance or any other type of risk. An effective system should safeguard the organisation's assets, facilitate internal and external reporting, and help the organisation comply with relevant legislation.

An internal control structure is comprised of:

- the control environment
- the internal controls themselves
- processes for monitoring effectiveness.

The control environment

An effective control environment is fostered by clearly stated policies and procedures and well-defined responsibilities and accountabilities that ensure the appropriate use of the organisation's assets.

A number of components are required, including the following:

- **Leadership** – Senior management provides a powerful role model in setting the ethical tone of the work environment and in maintaining an appropriate internal control culture. This is achieved through a participative and transparent management style that models, promotes and supports the desired culture. This includes setting and monitoring realistic goals, objectives and expectations. Managers should aim to demonstrate through their leadership, words and actions that they enforce and monitor the organisation's controls, and are themselves subject to those control constraints.
- **Organisational culture** – A culture that recognises the importance of supervisory accountability will reduce the incidence of fraud and corruption. (See Chapter 9).
- **Organisational structure** and **reporting structure** – A clear organisational and reporting structure ensures that every employee understands what they are responsible for and to whom they are accountable. This clarity also ensures that supervisors and managers understand their reciprocal obligations to monitor the activities, processes and outputs of their subordinates to ensure timely, accurate and quality work is produced in accordance with the control environment.
- **Delegations and approval processes** – The organisation needs to have clearly documented delegations and approval processes that are monitored. These place an emphasis on accountability, consistent with the focus of the FA Act.
- **Audit and risk oversight** (see Chapter 1 for more information.)
  - Internal audit is a valuable function which significantly strengthens the control environment. Departments are required under the FPMS (section 29(1)) to have an internal audit function. Statutory bodies are required to have one if so directed by the relevant Minister or by their board (FPMS section 29(2)). The internal audit function can be in-house or outsourced. In either case the organisation is still deemed to have an internal audit function. Any internal audit function must have a charter that is consistent with the auditing and ethical standards set by the relevant professional bodies (FPMS section 30).
  - An accountable officer must, and a statutory body may, establish an audit committee for their organisation, having regard for the guidelines, *Audit Committee Guidelines – Improving Accountability and Performance (2012)*, prepared by Queensland Treasury (FPMS section 35). An audit committee is designed to discuss issues identified by the internal and external audit functions and to provide independent advice to the accountable officer or statutory body.
  - The relationship between internal and external audit is also significant – it is important to recognise the limitations of the external audit function and the way it links with internal audit and compliance activities.
- **Employment of qualified and competent officers** – This requires adequate employment screening**.** A number of checks should be conducted before employing staff. These include: referee checks, verifying stated qualifications (particularly when qualifications are a requirement for a position), criminal history checks and disciplinary history checks. In addition, periodic checks of existing employees in high risk areas should be considered.

Department chief executives are required by Public Service Directive 07/11 – *Employment Screening*, to: (i) conduct employment screening for persons engaged, or proposed to be engaged, to perform relevant duties or prescribed duties in the Queensland public service, and (ii) implement a risk management strategy for agencies performing child-related duties.

The *Public Service Act 2008* (PS Act) Chapter 5, Part 6 (sections 150 to 186) provides for criminal history checks to be obtained and used as a means of determining employment suitability. These sections apply across a range of circumstances including regulated employment and child-related duties.

There are legislated screening requirements under the *Working with Children (Risk Management and Screening) Act 2000* for child-related employment, businesses and service providers. There are also specific requirements for the provision of services and care for people subject to the *Child Protection Act 1999*, the *Public Guardian Act 2014* and the *Family and Child Commission Act 2014*.

Organisations are obligated to conduct a full appraisal about the provision of services, the range of locations and circumstances in which these services may be provided, and implement appropriate responses where interaction with clients subject to the Acts discussed above can reasonably be anticipiated.

Where appropriate, a chief executive must also comply with screening requirements under Commonwealth and State legislation (e.g. security clearances and other background checking) which are not covered by the PS Act Part 6.

- **Code of Conduct** – This is a key document for describing the standards of conduct that are expected of public officers to ensure that their conduct is consistent with public sector ethics principles and values. The provisions of a code of conduct support many of the operational practices designed to minimise fraud and corruption risks. Public service agencies and public sector entities' codes are underpinned by the PSE Act, which makes contraventions of an organisation's code grounds for disciplinary action (PSE Act section 4). (See Chapter 8 for more information.)
- **Human Resources policies and practices** – These should anticipate the information needs of all employees and be written in plain English to provide clear, unambiguous guidance and standards. Information about the possible consequences of failing to adhere to the organisation's code of conduct, policies and practices should be made clear to staff.
  - The PSE Act section 24 gives directions regarding the basis for disciplinary action for contraventions of an organisation's code of conduct.
  - For the public service the grounds for discipline and the appropriate available disciplinary actions are specified in the PS Act, primarily in sections 186 to 192. The *PSC Guideline 01/17: Discipline* provides additional guidance on this.
  - For local government councillors, the LG Act applies.
  - Other organisations should develop separate written disciplinary policies and processes and give consideration to addressing conduct matters in performance agreement schemes.

Internal controls

Internal controls need to cover more than just an organisation's financial operations. They must cater for other aspects of operational performance, compliance and "corporate health".

Internal control systems should be designed to suit the individual organisation. Although many internal control practices have a common application, such as the separation of functions and a well-developed system of accountability, there is no "one-size-fits-all" set of internal controls that can simply be applied across all organisations.

To formulate controls for your organisation, begin with the identified set of fraud and corruption risks and proceed to an assessment of the possible internal control measures matching those risks. The use of control checklists may be helpful, but nothing substitutes for a detailed risk assessment and

treatment process tailored to the organisation and its operating environment. (See Chapter 2 for more information.)

Internal controls can take many forms. They can be simple procedures such as locking doors or limiting access, or processes that are built electronically into a system. They can also extend to more direct and intrusive supervision such as video surveillance of activities. Some of the most effective controls can be quite straightforward. For example, simply ensuring transparency of operations can have a powerful control impact, both internally and with external stakeholders. This could include placing details of tender processes and approved tenders on the organisation's website. The organisation's financial management practice manual is a control (FPMS section 16(3)(c)). More sophisticated controls may include data mining techniques that analyse expenditure patterns and uncover discrepancies in claims and payments.

Avoid having too many controls, or controls that are unduly restrictive. This can lower productivity and increase bureaucracy, thereby inviting noncompliance and shortcuts that increase risk. It is also pertinent to periodically test your controls to ensure they are working.

The *Australian Standard AS8001:2009* (p. 29) notes that the organisation's internal controls should be:

- appropriately documented
- subject to continuous improvement
- risk-focused
- effectively communicated to all stakeholders
- accessible to all personnel.

Processes must be documented and the documents must be readily available to all employees.
The organisation must provide employees with adequate and ongoing training in the processes.
The processes must be followed by the department or statutory body.

The following is a summary of some common types of internal controls.

Separation of duties – This is a well-known control principle that can be applied to nearly all business processes and systems, and is required under the FPMS (section 8) wherever practicable. It works by ensuring that no one person has complete control over all aspects of a transaction, record or resource. The separation of duties principle can be applied in various ways to many activities. It may involve physical access controls, the division of duties, or giving different security access levels for information.

Contractor screening – Using external providers of goods and services can be a high risk activity, and requires suitable controls such as pre-approval screening to reduce the risks. Consider pre-contract due diligence, reference and finance checks.

Contract management – For some high-risk externally provided goods or services, consider including contractual obligations that require the supplier and their staff to comply with your key integrity policies, such as the code of conduct, information security and gifts and benefits. Importantly, ensure that conflicts of interest provisions are included. If contracts are already established, review how the initial contacts with the provider were made and check for any possible conflicts of interest. Also conduct a risk assessment to identify other relevant controls.

For contractors in lower risk categories, giving them adequate information regarding the agency's policies and procedures and its code of conduct can also help by ensuring they know what is expected of them in their dealings with the organisation's staff. (See Chapter 10 for more information.)

All contractors should be advised that failure to adhere to these requirements will result in the contract being reviewed, which may well result in it being terminated. Additionally, if the contractor's conduct raises the suspicion that criminal action has occurred the matter will be reported to the appropriate authority (i.e. the QPS, and the CCC).

Information security systems – An organisation's information is a valuable asset that must be protected by a comprehensive fraud and corruption control program. This includes raw data and transaction records. Consequently, secure management of information resources lies at the heart of most organisations' operations. The increasing incidence of computer hacking makes this even more critical.

Management information and accounting systems are critical components of an organisation's internal control systems. Organisations must have control processes to ensure that the use of information is always legitimate, relevant and impartial in serving the public interest. Consideration must also be given to how that information is securely stored and processed, and how it is used in the organisation's decisions.

The Queensland Government *Information Standard 18: Information Security* (IS18) requires that organisations develop, document, implement, maintain and review appropriate security controls to protect the information they hold by:

- establishing appropriate information security policy, planning and governance within the organisation in line with this information standard, including adopting all specified frameworks, standards and reporting requirements
- ensuring appropriate security controls are implemented as detailed by this information standard and its supporting documents.

Internal controls are also essential to reduce the risk of inaccurate public records being created or public records being disposed of improperly. *Information Standard 40: Recordkeeping* (IS40) and *Information Standard 31: Retention and disposal of public records* (IS31) contain information on developing and implementing recordkeeping controls and protocols. Queensland State Archives can provide further guidance on strategies for developing and implementing these controls. The CCC Advisory, *Management of public records* provides information about the corruption risks associated with poor records management and strategies to prevent corruption.

Key controls include:

- an auditable log which records all instances of access to critical or sensitive information, and regular review of this log.
- processes to ensure that users' levels of access and combinations of access are appropriate for their role
- user-maintenance procedures, such as locking and deleting accounts when a person resigns
- controls over passwords, including requiring sufficiently complex passwords, regular password changes, and adequate checks before password changes are permitted
- adequate management of software patches (a poorly designed and implemented software patch, designed to fix problems, can sometimes introduce new problems)
- adequate integration or reconciliation where more than one system is in use
- regular tests to ensure your gateways, firewalls and security systems will resist hacking or disruption.

Controls for small organisations

In small organisations the practical arrangements for internal controls may differ. Hands-on management can provide good control and compensate for the absence of more formal control arrangements. For example, in some small organisations, even the board may need to take on additional oversight roles, such as approving cheque runs, or payment schedules.

Managers will often be able to identify incorrect data and significant variances from what they expect, and their direct knowledge of client concerns and informal communication can quickly draw attention to operating or compliance problems.

Small organisations may find it difficult to achieve an appropriate separation of duties. Whenever possible, duties should be assigned so as to provide suitable checks and balances. If this is not possible, management may need to supervise operations more directly. For example, expenditure authorisation might be restricted to the manager.

A manager needs to "reach down" further into the operational activities of a smaller organisation and carefully review supporting documentation, bank reconciliations, invoices, orders, bank statements and other matters. The way information is received and handled may need review; for example, certain external statements and confidential internal reports may need to be delivered in unopened envelopes to a manager.

The need for management to be more hands-on may also increase the risk of management overriding key controls. Accordingly, there also needs to be appropriate oversight from those charged with governance, i.e. the accountable officer, audit committee or board.

Other resources

More information on internal controls can be found in Queensland Treasury's publication, *Financial Management Tools*, 2012.

Another useful resource is the Committee of Sponsoring Organizations for the Treadway Commission (COSO) that sponsored a body of work that has resulted in many standard internal control terms. One of the most significant COSO developments was the issue in 2004 of the updated definitive study, *Internal control: integrated framework*. This work was revised and reissued in 2016 as the *Fraud Risk Management Guide.*

Responsibility for internal controls

The CEO carries ultimate responsibility for an organisation's system of internal controls, but still relies on the support of management in fulfilling this role through well-structured lines of accountability. Creating a suitable control climate is facilitated by clear lines of accountability and appropriate organisational structures, suitable value statements, unambiguous position descriptions and service protocols, and effective operating policies and procedures.

Everyone in the organisation has a role to play in making sure that internal controls are working properly.

Managers are primarily responsible for implementing the controls and monitoring their effectiveness.

Line managers and supervisors are often in the best position to identify system deficiencies that facilitate fraud and corruption. Their job descriptions should reflect this responsibility, including an ongoing obligation to ensure that staff know and comply with the internal controls relevant to their roles.

Every employee should contribute to the development of better systems and procedures that will improve the organisation's resistance to fraud and corruption. To realise this objective, they need to know about the risks faced by the organisation and be encouraged to develop and adopt effective controls. In addition to following and complying with the control systems, they should report every detected failure of those systems to their managers.

The Australian Auditing Standard ASA 240 – *The Auditor's Responsibilities Relating to Fraud in an Audit of a Financial Report* states:

> The primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the entity and management. It is important that management, with the oversight of those charged with governance, place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment. This involves a commitment to creating a culture of honesty and ethical behaviour which can be reinforced by an active oversight by those charged with governance. Oversight by those charged with governance includes considering the potential for override of controls or other inappropriate influence over the financial reporting process, such as efforts by management to manage earnings in order to influence the perceptions of analysts as to the entity's performance and profitability.

Accountability includes ensuring the operations of your controls, the expected standards of ethical and professional conduct, and the transparency of your decision making exceed the minimum standards set down by legislation and that the "spirit" underpinning these standards is willingly adopted rather than taken on as imposed.

The limitations of controls

Any control system is subject to limitations. There is always the risk that:

- a person will identify and take advantage of a control weakness
- two or more people may collude to circumvent the controls
- circumstances may cause a particular control to be omitted on cost–benefit grounds (a conscious risk treatment decision)
- errors of judgment may still occur, though effective controls will help detect and minimise any such occurrences
- a control will become ineffective over time due to changes in software, technology or organisational restructures, and that this will not be noticed.

It is not sufficient merely to have the controls in place. They must be exercised conscientiously and continuously, and not be allowed to fall into decay or disuse because employees are busy, overloaded or merely lazy. Every manager and supervisor has a primary responsibility to ensure that procedures and controls are followed faithfully.

An internal control system is not a guarantee of success, but it provides a cost-effective way of minimising fraud and corruption risks.

Monitoring effectiveness

The accountable officer or statutory body must ensure regular reviews of the systems used to manage the organisation's financial resources (FPMS section 15(3)). Continual monitoring and review of the organisation's internal control mechanisms should be part of the normal management process. Monitoring activities should feed into an annual reporting and audit program that assesses the controls and their effectiveness under any changed conditions or in the face of reported weaknesses.

Chief Finance Officers of departments are required under the FA Act section 77(2) and the FPMS section 57 to provide their Director-General with an annual statement on the effectiveness of internal controls. This type of reporting is highly recommended for all organisations.

The Queensland Audit Office states in its *Fraud Risk Management*, Report 9, 2013 that significant benefits can be gained by management running regular data analytics in a structured manner. Data analytics can quickly and efficiently uncover suspicious or anomalous patterns in transactions and can

examine large and complex data sets quickly, efficiently and consistently. Use of data analytics may, in itself, provide a deterrent to potential fraudsters.

The organisation's internal audit program should regularly review internal controls as well as auditing other more general procedural and compliance matters. To ensure an objective review that is beyond reproach, the organisation's audit program should be independent of any direct role in implementing internal controls or the fraud and corruption control program. These latter functions always remain a shared responsibility of line management.

If the organisation does not have an internal audit function, the need for one should be regularly reviewed. This can be done as part of the organisation's process for assessing the effectiveness of internal controls and evaluating internal compliance activities.

Reporting on controls

Each organisation should provide an annual statement of its risk management and control status, to reassure the public that all significant risk factors have been taken into account and that appropriate controls are operating. The level of disclosure needs to be comprehensive enough to give an accurate description of the organisation's operating environment. (See Chapter 10.)

The FPMS (section 49) directs that the requirements in the document, *Annual Report Requirements for Queensland Government Agencies* (prepared by the Department of the Premier and Cabinet) are adhered to. These requirements may change from year to year, but usually require agencies to disclose information about risk management, including providing reasons why an agency does not have an internal audit function.

Best-practice target

(1) The organisation should have a range of internal controls, designed to both prevent and detect fraud appropriate to its own operating environment and its specific risks.

(2) The organisation should systematically appraise its risk exposure, identify risks, and create control measures to deal with those risks. The control measures should be developed in conjunction with the risk identification and assessment process.

(3) The controls should be clearly documented in the financial management practice manual, policies and procedures and employees should receive training in these.

(4) The organisation should conduct appropriate screening of prospective employees for disciplinary and criminal history in addition to conducting referee and qualification checks. These checks should also be conducted before an existing employee is moved or promoted to a high-risk position.

(5) The organisation should conduct appropriate due diligence screening of prospective providers of goods and services. This should include a risk assessment and referee and finance checks.

(6) The organisation should use data analysis techniques as a detection tool, particularly in high risk areas.

(7) Management and employees should share the day-to-day responsibility for implementing and monitoring internal controls. Managers should bear the primary responsibility for leadership and for implementing and monitoring the control systems. Employees should follow and comply with the control systems and report every detected failure of those systems to their managers.

(8) The control systems should incorporate feedback and review functions that evaluate the effectiveness of the organisation's internal controls against updated risk assessments.

(9) The organisation's internal audit program should independently review the adequacy of the control arrangements on a regular basis.

(10) The internal audit function should develop a strategic internal audit plan appropriate to the size and functions of the organisation to provide an overall strategy for the internal audit function for a period of at least one year, and an audit program that sets out the audits it intends to carry out during the year (FPMS section 31).

Additional reading

- CCC Advisory 2017, *Management of public records*, CCC Brisbane
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management: Integrated Framework*, 2004.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Fraud Risk Management Guide*, 2016
- Queensland Audit Office 2012, Auditor-General of Queensland Report 5: 2012 *Results of Audits: Internal control systems*, QAO Brisbane. <www.parliament.qld.gov.au/Documents/TableOffice/TabledPapers/2012/5412T401.pdf >
- Queensland Treasury 2012, *Internal Controls training*. <http://treasury.govnet.qld.gov.au/internal-controls>

Checklist: Internal controls

The following questions are indicative only. Each organisation should develop its own checklist to reflect its specific needs and risk environment. The checklist should be re-examined and updated periodically, as part of the organisation's program of fraud and corruption control appraisal.

Legislative requirements

- ☐ Have appropriate internal control measures been implemented to deal with all the identified fraud and corruption risks? (FA Act section 61, FPMS section 8)
- ☐ Is there appropriate separation of duties between officers of the organisation? (FPMS section 8(6))
- ☐ Is the internal control structure included in the organisation's FMPM? (FPMS section 8(5))
- ☐ Does the organisation review its internal controls system regularly enough to cater for changing circumstances? (FPMS section 15(3))
- ☐ Are the delegations, authorities and supervisory roles of management clearly defined? (FPMS (8)(2)(b)(i)
- ☐ Is there an internal audit function? (FPMS section 29.)
- ☐ Does the internal control structure include appropriately qualified officers? (FPMS section 8(2)(b)(ii))

Recommended Best Practice

- ☐ Are there systems or procedures to regularly monitor and evaluate the controls?
- ☐ If there have been any major changes to the organisation structure, functions or operating environment, have internal controls been reviewed for ongoing adequacy?
- ☐ Are the responsibilities for fraud and corruption control clearly documented in organisation policies, procedures and job descriptions?
- ☐ Does the organisation actively involve senior executives and line managers in reviewing operational practices and controls to prevent and detect fraud and corruption?
- ☐ Have all stakeholders been made aware of the risks and organisation control mechanisms?
- ☐ Do the organisation's contracts with suppliers require the supplier and their staff to comply with the organisation's key integrity policies?
- ☐ Are line managers and employees made aware of the content of policies and procedures and controls relevant to their roles and to fraud control?
- ☐ Are the managers aware of their obligation to ensure their staff know and implement the internal controls relevant to their role?
- ☐ Do the employees in these positions consciously accept their control responsibilities?
- ☐ Does each work unit or business process comply with all policy obligations for delegations and organisational review?
- ☐ Does the organisation conduct checks on prospective employees' references, stated qualifications, criminal histories and discipline records?
- ☐ Are organisation delegations routinely reviewed and employees advised of relevant changes?
- ☐ Does the organisation regularly check for duplication, overlap, conflict or lack of coverage that is likely to reduce the effectiveness of the organisation's fraud and corruption controls?
- ☐ Does the organisation implement routine data analytics in areas identified as inherently susceptible to fraud?

- ☐ Are managers and employees consulted about specific investigations which may involve any control lapses in their areas of operation?
- ☐ Do any supervisors affected by changes in controls review the interim or final investigation reports as part of their obligations to understand and apply the anticipated changes?

Chapter 4 – Reporting processes

The topics covered in this chapter are:

(1) The value of reports of wrongdoing
(2) The legislative requirements
(3) Challenges to reporting
(4) Reporting policies and procedures
(5) Reporting systems
(6) Encouraging reports from inside the organisation
(7) Encouraging reports from outside the organisation
(8) The role of management
(9) Evaluating effectiveness
(10) Best-practice target

The value of reports of wrongdoing

The reporting of suspected misconduct and maladministration within the Queensland public sector is fundamental to its ongoing integrity and health.

Research studies and surveys consistently show that reports by employees are one of the most common ways that fraud and corruption are discovered. Research by Brown, Mazurski and Olsen identified that "Reporting by employees ranked overall as the single most important trigger for the uncovering of wrongdoing." (2008, p. 44.)

KPMG Fraud and Misconduct Surveys have consistently revealed that employees were responsible for detecting a significant number of fraud incidents within their organisations. The longer it takes for a fraud to be identified the further the fraud can escalate and the more damage an organisation is likely to suffer. This may lead to significant impact in terms of financial loss and reputational harm. The KPMG *Fraud, Bribery and Corruption Survey 2012: Australia and New Zealand* reported that it could take up to 665 days to detect a fraud (p. 3).

One of the reasons it can take so long for a fraud to be detected is the time it takes for people to decide to report their suspicions to the appropriate person or organisation. An effective reporting system that encourages and enables people to report is a powerful tool in assisting with the early discovery of fraud and corruption.

The benefits to an organisation of implementing reliable and trusted reporting systems which will capture reports of wrongdoing from internal and external sources include:

- identifying wrongdoing earlier
- exposing weak systems that may make the organisation vulnerable to loss or legal action
- avoiding financial loss and inefficiency
- maintaining a positive corporate reputation
- improving accountability
- deterring staff from engaging in improper conduct.

All organisations should have ways for people to report suspicious actions or possible wrongdoing. In addition, there are legislative requirements for establishing and maintaining a system for reporting certain types of matters.

The legislative requirements

The *Financial Accountability Act 2009* (section 61 and section 77) establishes that the accountable officer or statutory body is responsible for establishing, maintaining and reviewing financial internal controls, with responsibility delegated to the CFO in departments.It is important to remember that effective internal controls may be ignored or bypassed by a motivated fraudster. Alternatively, an internal control may not work and therefore does not provide the safeguards expected. Internal controls should therefore be complemented by a mechanism that will encourage people to report any apparent internal control failure, or suspicion of fraud or corruption.

Departments or public service offices as defined by the *Public Service Act 2008* are required to comply with the PSC *Directive 02/17: Managing Employee Complaints* which requires them to implement and maintain an employee complaints management system. Failure to have a functional reporting system for employee complaints will be a breach of this Directive.

Agencies whose complaints management system does not function well or is not widely understood and followed run the risk that complaints might become systematically suppressed, which is a form of organisational corruption. Deliberate suppression of complaints by individuals is potentially a criminal act.

Where the reporting of fraud or corruption amounts to a public interest disclosure (a PID), the *Public Interest Disclosure Act 2010* (PID Act) will also apply. Under section 28, the CEO must establish reasonable procedures to manage any PIDs. In addition, while many Acts require that confidentiality be maintained, the PID Act section 37 states that a person who makes a PID is deemed to not be committing an offence under any Act that otherwise imposes a duty to maintain confidentiality.

The *Code of Conduct for the Queensland Public Service* states that "As part of demonstrating our commitment to uphold this Code, we need to identify and report conduct that is not consistent with this code." Any fraudulent or corrupt conduct will fall into this category.

For public sector organisations not covered by the *Code of Conduct for the Queensland Public Service*, the importance of reporting can be emphasised by including a provision within the organisation's code of conduct requiring all officers to report any suspected fraud, corruption or maladministration of which they become aware, and failing to do so may make them subject to discipline.

Challenges to reporting

Loyalty to organisations, work units and colleagues is encouraged; however, loyalty may be misplaced if it covers up wrongdoing, and this kind of loyalty is not in the public interest.

There are a number of factors that can make reporting very difficult for the individual.

- **Clash of values between commitment to the public interest and loyalty to colleagues** – Australian culture places a high value on protecting mates in trouble. This sense of loyalty can lead people to put aside what should be the overriding commitment to the broader public good.
- **Fear of retribution or victimisation** – People who have exposed corrupt conduct, fraud, and corrupt or criminal behaviour should have been applauded, but some of them have suffered criticism, lost friendships, lost career prospects and even their jobs.

- **Concerns of breaching confidentiality requirements** – Commercial confidentiality is commonly quoted in contractual matters, and employment contracts increasingly contain confidentiality clauses making the unauthorised disclosure of information a disciplinary matter. The statute books carry many references dealing with the unauthorised release of confidential information, but are generally silent in respect of any public interest defence. These strict rules can create the false impression that fraud matters linked to important information cannot be disclosed under any circumstances.

To help overcome resistance and to encourage reporting, organisations need to be forthright in stating that they want people to denounce unethical and fraudulent behaviour. The organisation also needs to provide clear guidance to employees on how to deal with an ethical dilemma when faced with potential wrongdoing.

Staff and managers also need to encourage reporting. This requires that they understand how to report wrongdoing and, where appropriate, are able to contribute to increasing the effectiveness of management reporting processes.

To support reporting, the organisation needs to have clear policies, procedures and systems, as well as training and communication about them.

Reporting policies and procedures

Organisations should have policies and procedures that encourage and enable people to report fraud and corruption. This may stand alone or form part of a more general reporting policy covering the full range of reporting requirements.

Whichever is the case, the policy and procedures should include:

- what constitutes reportable conduct, behaviour or risks
- who can make a report
- how, when and where to make a report
- to whom a report should be made
- what should be done by the person receiving the report
- how the reports are documented and the records managed
- how false, vexatious or mischievous reports will be dealt with
- the processes for assessment and investigation of disclosure allegations
- procedural arrangements for appropriate responses and feedback to the complainant about the organisation's progress in handling the complaint. These arrangements should include details about how often feedback is provided, what is included, and a requirement to provide a written reply to the complainant when the matter is concluded
- a guarantee of fair and objective treatment of everyone involved
- a commitment to protect any relevant parties from reprisals
- available support and protection mechanisms
- the role and responsibilities of management.

All stages of the reporting process must be adequately documented. Every report must be able to be traced from initial receipt, through the organisation's process for investigation, follow-up and resolution, to notification to the complainant and any relevant internal oversight committees, and to providing information for annual reporting purposes. There should also be processes to remind key personnel (e.g. "bring-up" reminders) to ensure reports are processed within acceptable timeframes.

The Office of the Queensland Ombudsman, as the oversight agency under the PID Act, has developed a Model Public Interest Disclosure Procedure to assist agencies fulfil their legislative obligations.

Reporting systems

To encourage reporting, arrangements for reporting need to be flexible, and to provide an open and receptive process that gives potential complainants confidence in the system. For example, if a person thinking about making a report is concerned about an open approach to a supervisor or nominated disclosure officer, they should be able to request a meeting away from the workplace, make a complaint anonymously, or go to an external body such as the CCC (see Chapter 6).

A good reporting system needs to include mechanisms to:

- receive information about identified risks and suggestions for system improvements
- receive information about suspected acts of fraud and corruption, including anonymous reports
- maintain the confidentiality of the parties involved as far as is possible
- pass information on to an appropriately authorised officer (usually but not always the supervisor or manager)
- ensure appropriate assessment and investigation
- ensure compliance with additional external reporting requirements
- provide feedback to the informant, demonstrating that the information was taken seriously and acted upon
- be a reliable means of gathering information for analysis so that trends and issues can be examined over time and acted upon.

Reporting from both inside and outside the organisation will increase if a range of channels for reporting is provided.

Hotlines

A hotline is usually a dedicated email address, a telephone or facsimile number that gives people a means of contacting the organisation anonymously. This serves both deterrent and control functions.

A hotline arrangement enables people with information or concerns to communicate those concerns and obtain advice before making decisions that may have significant legal or ethical implications (such as the making of a PID).

A hotline has the advantage of being perceived as being independent of management. This perception can be enhanced, and 24-hour access provided, by using a third-party provider (e.g. by outsourcing the hotline to a specialist professional group or a central liaison body). Affiliated organisations or groups, such as smaller local governments, may find such an approach useful.

Anonymous reports

Anonymous complaints can be a rich source of information. This is why providing a mechanism for people to report anonymously is so valuable. Making a report about any form of wrongdoing can be very challenging for some people so it is important to reduce the stress associated with this action. Having made the report an anonymous discloser is unlikely to make further contact. Therefore, it may not be possible to contact the anonymous reporter to subsequently verify details or seek further information about the initial report. That is why it is important that organisations ensure that their systems are set up to capture as much information during the initial report as possible.

Reporting to other organisations

There may be factors that inhibit or limit the effectiveness of internal reporting processes, such as situations where the wrongdoing appears to involve senior management, or where there is concern about how the matter may be handled. Some employees may find internal reporting too stressful to

allow them to speak up openly. Internal systems also may not suit external parties who want to report their suspicions.

Organisations need to make people aware that complaints can be made directly to other organisations. For example, complaints about maladministration can be made directly to the Ombudsman, and complaints about corrupt conduct in UPAs can be made directly to the CCC. (See Chapter 6 for other external reporting options.)

Encouraging reports from inside the organisation

For an employee to make a report about wrongdoing, simply having a reporting system is not enough. Employees need to feel confident about using the reporting mechanisms. This confidence will come from readily accessible and well publicised systems that encourage people to take appropriate action, secure in the knowledge that supporting arrangements will protect individuals and preserve their confidentiality as far as possible. (See Chapter 5 for more information about supporting and protecting people who report wrongdoing.)

The organisation also needs to make employees aware of all the available reporting procedures. Guidelines on how and where to report suspected fraud and corruption should be part of the organisation's complaints policy or ideally outlined in a separate reporting policy document.

The success of the reporting system will be determined by how it is perceived. It should be seen to operate fairly and objectively regardless of the source of the report. It is also important to demonstrate to staff that their concerns will be treated seriously and objectively, and this can be achieved by establishing a recognised neutral party within the organisation to receive reports — for example, an ethics or compliance officer or other suitably qualified senior manager.

The size of the organisation will dictate the nature of the reporting system. A larger organisation might have a dedicated corporate integrity or ethical standards unit, as well as specific officers and a hotline dedicated to receive and deal with initial reports. In a small organisation direct reporting to the accountable officer or CEO may be appropriate. It is also important to take account of the organisation's structure, function and geographic reach.

Under normal circumstances, reporting should be to immediate supervisors or managers in the first instance, and so the internal reporting system should encourage a free flow of information through the normal supervisory and management channels. Supervisors, in turn, are responsible for reporting to more senior management. The most effective way to encourage this process is through the development of a climate of trust and accountability in which employees know that confidentiality will be maintained (as far as possible) and that appropriate action will be taken to deal with their concerns.

In some cases, employees may be reluctant to report their concerns to an immediate supervisor, even if the complaint does not involve that person. Alternative reporting channels should therefore be accepted, such as reporting to a more senior manager, a nominated receiving officer, a corporate integrity unit or the CEO, or through a hotline, and should include mechanisms for reporting anonymously.

When initial reporting is not directed to the CEO, the receiving officer(s) must have an unrestricted line of access to the CEO. This is because the CEO has legislative responsibility for reporting to external bodies in particular circumstances (CC Act, section 38), and consequently the CEO must ensure that there are appropriate arrangements to receive timely and effective advice of any likely reportable situations so that they can fulfil this obligation. (See Chapter 6 for more information.)

The willingness to report depends on an awareness of the significance and adverse impact of fraud and corruption and the ability to recognise whether some observed behaviour is inappropriate or not. Ignorance and uncertainty can discourage an individual from reporting, especially if others in the workgroup or elsewhere in the organisation condone or ignore the activity. A common understanding

of public sector ethics principles and typical indicators of fraud and corruption should be developed through a code of conduct and suitable training and awareness programs. (See Chapters 8, 9 and 10 of these guidelines.)

Encouraging reports from outside the organisation

People outside the organisation can also become aware of fraud or corruption occurring in a government organisation. In particular, this might include suppliers, contractors and consultants providing goods or services to the organisation, third party providers of services delivered on behalf of the government to clients and customers, and clients themselves, including members of the public generally, not-for-profit organisations and other businesses.

To encourage reporting from outside parties, organisations should make their fraud and corruption control policy available to all of these groups, and provide them with access to information in relation to their rights, responsibilities and obligations including information on their responsibilities for fraud control. Commonly, clear statements encouraging the receipt of reports and how to make them are posted on the organisation's website to encourage people to come forward if they have information.

It is important that the organisation have clear processes in place that are flexible enough to take into account a variety of report types. For example, reports on fraud or corruption may arrive in the form of a service complaint or a suggestion for improvements to service.

The role of management

Managers play a key role in the reporting process. They help to set the organisational tone and lower the perceived barriers to reporting. They may receive and deal with a complaint; they may be involved with a resulting investigation; and they carry the primary responsibility for forestalling any potential reprisals within the work group. The significance of the manager's role has been highlighted by research into factors that shape employees attitudes to reporting (Roberts et al. 2009).

Employee relationships are crucial in the aftermath of a report and managerial leadership does much to set the workplace climate. The line manager is also uniquely placed to anticipate employees' responses to a report and subsequent investigation activities.

Managers and employees must never act in a way that could be seen as victimising or harassing a discloser. They must also protect and maintain the confidentiality of any person known or suspected to have made a report, particularly if the report is classified as a public interest disclosure (PID). (See Chapter 5 for more information.) Confidentiality is an important factor in minimising reprisals. If part or all of the disclosure does become known, early intervention is important in minimising employees' negative reactions and preventing possible reprisals towards the discloser.

Other aspects of the manager's role in relation to a report are to:

- minimise the stress on a discloser and provide suitable encouragement when they make a report
- undertake a risk assessment and implement appropriate risk management strategies to cater for likely fallout from a report
- provide constructive leadership to the workgroup during any investigation
- work closely with human resources and other units to ensure the necessary level of support and protection
- ensure the preservation of all information and materials that might be needed as evidence
- provide timely and appropriate feedback to all relevant parties (where possible)

- behave in a manner that acknowledges that the subject of a report is also entitled to support and the presumption of innocence until the matter is settled and decided.

Managers must act with integrity and impartiality and overcome any personal concerns in meeting their obligations, especially if the allegations reflect adversely on their group. While counselling employees not to make false or malicious allegations, managers must still be alert to the "red flags" of potential fraud and corruption and carefully examine all allegations. They must fulfil their managerial roles fairly and objectively, no matter how difficult.

Evaluating effectiveness

A close examination of reported incidents, and other sources of ad hoc and regular reporting (e.g. internal audit, external auditor, management committees) can often show more deep-seated systemic or managerial problems, and reports and more formal complaints are good indicators of where to look. In conjunction with regular internal audit, an incident analysis can provide a useful insight into the effectiveness of the reporting process and organisational health. The incidence of reports and trends identified may enable actionable targets to be set, as an incentive to improve control systems and ultimately minimise the opportunities for fraud and corruption.

Checking the user-friendliness and effectiveness of the reporting system from time to time helps to gauge the program's value. Past records will generally show whether people believe they are encouraged to report, and whether they have developed greater confidence in the process as a result of the response they received.

Surveys of employees, clients, suppliers and other groups are useful in assessing their willingness to use the available reporting arrangements.

Calls to a hotline depend on the initiative of individuals, so a review of the number and content of calls can indicate the effectiveness of the system.

Best-practice target

(1) The organisation should have a reporting system with a variety of robust mechanisms for reporting suspected fraud and corruption, including anonymously and to an external contact.

(2) The system should be supported by an appropriate policy that informs and encourages stakeholders to report wrongdoing.

(3) The system should be reflected in well-developed procedures for dealing with each step in managing a report.

(4) The Code of conduct should require employees to report suspected wrongdoing, including fraud and corruption.

(5) Managers and supervisors should be trained in how to recognise and handle reports.

(6) The reporting arrangements, rights, responsibilities and obligations should be communicated to all stakeholders, both internal and external.

(7) Executives and managers should demonstrate commitment to support reporting of wrongdoing, so that reporting becomes something that is both expected and accepted, and is seen as a continuing and shared responsibility of employees and management.

(8) Information from all stages of the process should be properly recorded.

(9) The information recorded should be regularly analysed to identify fraud and corruption trends.

(10) The effectiveness of the internal reporting systems should be regularly examined against updated risk assessments through suitable feedback and review activities.

Additional readings

- Brown, AJ, Mazurski, E and Olsen, J 2008, *Whistleblowing in the Australian Public Sector*, ANU Press, Canberra. <http://epress.anu.edu.au?p=8901>
- G20 Anti-Corruption Action Plan Action Point 7: *Protection of Whistleblowers*, 2011. <www.oecd.org/g20/topics/anti-corruption/48972967.pdf>

Checklist: Reporting processes

The following questions are indicative only. Each organisation should develop its own checklist to reflect its specific needs and risk environment. The checklist should be re-examined and updated periodically, as part of the organisation's program of fraud and corruption control appraisal.

Legislative requirements for departments or public service offices as defined by the *Public Service Act 2008*

- ☐ Has the department implemented and is it maintaining an employee complaints management system as required by the PSC *Directive 02/17: Managing Employee Complaints*?

Recommended Best Practice

- ☐ Does the organisation have a reporting system with a variety of robust mechanisms for reporting suspected fraud and corruption, including anonymously and to an external contact?
- ☐ Does the Code of conduct require employees to report suspected wrongdoing, including fraud and corruption?
- ☐ Does the organisation have an appropriate policy that informs and encourages stakeholders to report wrongdoing?
- ☐ Does the organisation have well-developed procedures for dealing with each step in managing a report?
- ☐ Does the organisation have a process whereby outsiders can report corrupt conduct to the organisation?
- ☐ Does the organisation encourage the reporting of fraud and corruption issues such as:
  - ☐ potential or actual risks
  - ☐ areas for improvements
  - ☐ suspect behaviour?
- ☐ Has the organisation made employees aware of its fraud and corruption policy and procedures?
- ☐ Has the organisation nominated particular officers or positions to receive reports?
- ☐ Are receiving officers or positions appropriate for the reporting role, given the organisation's structure and the nature of its business, client base and employees?
- ☐ Are receiving officers trained to recognise and handle reports?
- ☐ Do employees know what to expect once they have submitted a report?
- ☐ Does the organisation carefully review and monitor all complaints and reports?
- ☐ Are individuals (if known) informed about the outcome of their report, including, if applicable, why an investigation might not have proceeded?
- ☐ Does the reporting system ensure that appropriately serious allegations are reported to the CEO?
- ☐ Do organisation records indicate that reports of fraud and corruption have been considered at an appropriately senior level?
- ☐ Is strict confidentiality maintained in the receipt and processing of reports?
- ☐ Does the organisation have an effective information management system that captures all reports and enables evaluation of the anti-fraud and corruption program's effectiveness?
- ☐ Does the organisation have a hotline service to provide information to people with concerns, and is the hotline advertised?

Chapter 5 – Protections and support for disclosers

The topics covered in this chapter are:

- How protections support fraud and corruption control
- The legislative framework
- Roles and responsibilities
- Recommended protections and support
- PID specific requirements
- Best-practice target

How protections support fraud and corruption control

Employees are often reluctant to report for fear of retribution.

Many organisations have been slow to encourage those who know about wrongdoing to come forward. Instead of being applauded, employees who have exposed corrupt conduct, fraud, and corrupt or criminal behaviour have suffered criticism, lost friendships, lost career prospects and even their jobs. These employees often find their stress levels rise and their health suffers. In some cases victimisation and retribution can include physical violence against themselves and their possessions.

This issue has received international recognition, and at the Seoul Summit in November 2010, G20 Leaders identified the protection of whistleblowers as one of the high priority areas in their global anti-corruption agenda (G20 2011, p. 2).

Providing protections for whistleblowers helps to reduce employees' fears of retribution.

The legislative framework

Work Health and Safety Act 2011

Organisations have a responsibility to ensure the health and safety of their staff. Failing to take this responsibility seriously is a breach of the *Work Health and Safety Act 2011*.

Crime and Corruption Act 2001

Many reports of fraud or corruption will be classified as reports of corrupt conduct as defined in the *Crime and Corruption Act 2001* (CC Act). The CC Act includes provisions to protect those who make reports of corrupt conduct.

Public Interest Disclosure Act 2010 and *PID Standard No. 1*

Some reports about fraud and corruption will be classified as a public interest disclosure (a PID). A PID is a disclosure of information as a result of a genuine concern about the possible serious wrongdoing of public officers, or of others who may be acting in a way that is not in the public interest. The definition depends on who is making the disclosure, with the *Public Interest Disclosure Act 2010* (PID Act) distinguishing between disclosures made by a public officer and those made by anyone else. For a report about possible fraud and corruption to be treated as a PID, it must meet the definition in the PID Act sections 11 to 13.

A person who discloses this information is referred to as a "discloser". Previously, people have used the term "whistleblower." The discloser of a PID is offered special protections under the PID Act to protect them from reprisals.

The underlying grounds for a PID come principally from the government's ethics framework (i.e. the overarching policies, Acts and directives of government), together with the organisation's code of conduct and subsidiary policies. The *Public Sector Ethics Act* (PSE Act) and the *Public Service Act 2008* (PS Act) provide the legislation for the ethical framework and outline the principles of public sector conduct and guidelines for the types of behaviour that are acceptable. Failure to comply with these requirements may constitute reportable conduct within the meaning of a PID.

The PID Act aims to facilitate the disclosure of wrongdoing by providing protections for those who make disclosures. It sets out what may be disclosed as a PID and the pathways for making disclosures, and establishes strict confidentiality requirements for PID management.

While many Acts require that confidentiality be maintained, the PID Act section 37 states that a person who makes a PID is deemed to not be committing an offence under any Act that imposes a duty to maintain confidentiality.

In Queensland PIDs are overseen by the Queensland Ombudsman who has the authority to set standards for the management of them. *Public Interest Disclosure Standard No. 1* details the actions each CEO of a public sector entity must take to ensure that their agency:

- implements a management program, including policies and procedures, for responding to public interest disclosures
- has procedures for receiving, assessing and managing public interest disclosures
- protects the confidentiality of disclosers, subject officers and other persons involved
- provides support for disclosers
- undertakes risk assessments and action to prevent reprisal against disclosers and other persons involved in public interest disclosures.

More detailed information about the legislative responsibilities of individuals, managers and organisations is provided in the three *Public Interest Disclosure User Guides* which are available from the Queensland Ombudsman's website <www.ombudsman.qld.gov.au>.

Roles and responsibilities

The organisation must show, through words and actions, that it will take all reasonable steps to provide support to disclosers and protection from reprisal as a result of a disclosure.

Organisational responsibilities

The organisation should have established procedures for protections and support for disclosers so that people know what to do when the need arises. To ensure that the organisation's support and protective mechanisms are always active, responsive practices need to be embedded within the organisation's procedural framework. For example, everyone should know that suspected fraud or corruption should be reported immediately to a supervisor, manager or nominated officer, or to the CEO. (See *Public Interest Disclosure Standard No. 1*.)

The PID processes will supplement the usual processes surrounding reporting, such as grievance procedures or complaints related to discrimination, harassment, bullying and similar workplace issues for which there should also be specific procedures.

Managers' responsibilities

A report about any kind of wrongdoing is a serious matter; however, any report may contain information about a potential PID. This is why organisations should ensure that every manager is trained about how to identify and deal with a PID, even in circumstances where the discloser may not be aware that their complaint contains a PID.

Once it is determined that a complaint may contain a PID the officer receiving the disclosure is to ensure the discloser fully understands:

- the limitations regarding the privacy of a complaint – while a disclosure must be taken and reported confidentially, the subsequent handling and investigation of the subject matter will mean that the organisation cannot guarantee the confidentiality of either the discloser or the material disclosed
- the likely outcomes of the disclosure and reporting process
- the implications for the discloser should their information be assessed as a PID
- what to expect in the way of organisational support and protection.

At the commencement of taking a complaint about alleged wrongdoing the officer receiving the complaint may not know it contains a potential PID. Therefore, as a best-practice minimum, and to anticipate the requirements of a report subsequently being determined as a PID, it is recommended that all information and reports be documented. In the event that the disclosure is made orally, the receiver will need to summarise the details in writing at the earliest opportunity.

Receivers need to be careful not to take any action likely to jeopardise an investigation or be seen as self-interested, so that there can be no grounds for any perception that there has been an attempt to cover up, influence or prejudice the outcome of an inquiry.

As employees move into the supervisory and management ranks, they should receive more specialised training to improve their ability to receive and deal with reports of wrongdoing, including the development of skills in providing appropriate support and protection. (See *Public Interest Disclosure Standard No. 1* for specific requirements.) (See Chapters 9 and 10 for general education and awareness issues, and Chapter 7 regarding the training needs of investigators.)

Protections and support

Under the *Workplace Health and Safety Act 2011* (WHS Act), all organisations are required to ensure the wellbeing of its staff and of members of the public. Reports about wrongdoing may not immediately raise a suspicion that the matter may be a PID; therefore, all reports should be treated as a PID until the organisation is certain. This includes ensuring that appropriate protection measures also apply to people external to your organisation. It is important that your organisation's policies and procedures provide protection measures for any person making a complaint and that your employees understand their obligations when receiving a report.

As soon as possible after receiving a report, the organisation should determine the appropriate level of protection and support for the discloser by conducting a risk assessment. This process should consider the risk of reprisal to the discloser and others associated with the discloser. It must also determine the discloser's need for support and the organisation should ensure protective measures proportionate to the risk are in place.

The discloser should be given specific advice and guidance about their own behaviour in the workplace. In particular, this should include the need for the discloser to observe confidentiality requirements. Deliberate or inadvertent release of information could jeopardise an investigation, and could increase the likelihood of reprisals.

It may be appropriate for the organisation to nominate a contact officer for the discloser. For public officers, a discloser's direct manager is usually well placed to act as a support to the discloser (unless the manager is excluded from this role because of involvement in the disclosure or investigation). Alternatively, it may be more appropriate to appoint a manager in another area as their contact officer. Ideally, the discloser should be consulted about the choice of a support officer. During the process, the entity will need to continue to review the discloser's situation and it may be necessary to revise the support arrangements. Whilst best practice for all reports, this review process is an obligation placed on the CEO if the report is a disclosure under the PID Act.

Other measures likely to contribute to successful support and protection include:

- a case-specific formal program or a support network that comes into operation once a report is made. These may involve designated case managers and/or support officers
- management of issues by specially trained investigative employees or human resource specialists, if required
- counselling and other forms of emotional support
- informal support networks through liaison with other disclosers (where appropriate), and line managers.

It is not only disclosers who may be affected by reports of wrongdoing. Safeguarding the rights of any person who is the subject of, or is in some way associated with, a disclosure is equally important and demonstrates the organisation's resolve to treat disclosures appropriately. Managing the whole process equitably will increase employee confidence and improve the likelihood of responsible reporting.

PID specific requirements

Under the PID Act, public sector entities' CEOs have obligations to establish reasonable PID procedures to ensure that:

- the entity has a management plan for dealing with PIDs
- public officers who make disclosures are given support and offered protection from reprisal
- PIDs made to the entity are properly assessed and, where appropriate, investigated and dealt with
- appropriate action is taken in relation to wrongdoing that is the subject of a PID.

The PID Act section 28 (2) requires public sector entities to publish procedures on their websites, and to make them accessible to the public. Compiling a plain English "how to make a PID" guide is also recommended.

When a disclosure has been made, the PID Act requires that the discloser be provided with confirmation of the receipt of the PID and a description of the action taken (or proposed to be taken). If the organisation believes no action is required, the discloser must be advised of this in writing and the reasons for this decision must be given.

As soon as possible after receiving a PID, the CEO must determine the level of protection and support appropriate for the discloser by conducting a risk assessment. This process should consider the risk of reprisal to the discloser and others associated with the discloser. It must also determine the discloser's need for support, and the CEO must ensure that protective measures proportionate to the risk are in place. During the PID process, the entity will need to continue to review the discloser's situation and it may be necessary to revise the support arrangements.

It is not necessary for the person to identify the disclosure as a PID when making it. It is the agency's obligation to identify whether the allegation meets the PID requirements and take action accordingly.

The Ombudsman also has an obligation to provide or coordinate the provision of education and training about PIDs. (See Public Interest Disclosure Standard No. 1.)

The information in this chapter is provided as a guide, and does not cover all the components of an effective PID program. Further information is available from the Queensland Ombudsman and the CCC (CMC, QO, PSC 2011) (Also see Chapter 4 on Reporting systems.)

Best-practice target

(1) The organisation's policy and procedures should encourage people to come forward and report suspicions of maladministration or fraud and corruption.

(2) The organisation's PID arrangements should provide robust support mechanisms; minimise the likelihood of false or misleading reports; offer guidance on appropriate behaviour by disclosers; and ensure protection against reprisal as a result of a disclosure.

(3) The organisation's PID reporting structure should reflect the size, structure and nature of the organisation, its constituent work units and the staffing profile, and must be consistent with the regulatory regime.

(4) Details of the organisation's PID policy and reporting structure should be widely disseminated to stakeholders including staff who comprise potential disclosers.

(5) The organisation should treat all reports of wrongdoing as PIDs unless and until it is certain that it is not.

(6) Education and awareness programs should be provided to ensure that PIDs are handled suitably, and that supervisors and managers properly fulfil their roles in disclosure support and protection.

Additional readings

- *Public Interest Disclosure Act 2010*
- Public Interest Disclosure Standard No. 1
- Queensland Ombudsman's website includes the following:
    - How to manage a public interest disclosure <www.ombudsman.qld.gov.au/improve-public-administration/public-interest-disclosures/how-to-manage-a-public-interest-disclosure>
    - Managing a public interest disclosure program: A guide for public sector organisations
    - Making a public interest disclosure: A guide for individuals working in the public sector
    - Handling a public interest disclosure: A guide for public sector managers and supervisors <www.ombudsman.qld.gov.au/improve-public-administration/public-interest-disclosures/public-interest-disclosure-resources/public-interest-disclosure-guides>

Checklist: Protections and support for disclosers

The following questions are indicative only. Each organisation should develop its own checklist to reflect its specific needs and particular risk environment. The checklist should be re-examined and updated periodically, as part of the organisation's program of fraud and corruption control appraisal.

Legislative requirements

- ☐ Does the organisation have written PID procedures? (PID Act section 28)
- ☐ Do the PID procedures cover:
  - ☐ support and protection available for the discloser of a PID?
  - ☐ how to assess a disclosure?
  - ☐ the investigative process?
  - ☐ employee and management responsibilities? (PID Act section 28 (1))
- ☐ Are the PID procedures published on the organisation's public website? (PID Act section 28 (2))
- ☐ Are there systems in place to support, protect and communicate with disclosers? (PID Act section 28)
- ☐ Is there an appropriate internal review mechanism for any discloser who may feel they have been disadvantaged or subjected to reprisals? (PID Act section 28 (1) (e))
- ☐ Are disclosers (if known) informed about the outcome of the disclosure and inquiry process, including why an investigation might not have proceeded (if applicable)? (PID Act section 30 (3))
- ☐ Does the organisation have a process for recording PIDs and their outcomes? (PID Act section 129)
- ☐ Does the organisation have a nominated officer or work unit responsible for PID management? (PID Standard No. 1)
- ☐ Does the organisation provide education and training about PIDs? (PID Standard No. 1)
- ☐ Does the organisation report on the outcomes of PID Activities in accordance with the requirements set by the Queensland Ombudsman? (PID Act section 33)
- ☐ See also the Queensland Ombudsman's Self-assessment checklist <www.ombudsman.qld.gov.au/improve-public-administration/public-interest-disclosures/how-to-manage-a-public-interest-disclosure/does-your-pid-policy-measure-up/does-your-pid-policy-measure-up>

Recommended Best Practice

- ☐ Does the organisation have a stand-alone PID policy?
- ☐ If there is a stand-alone PID policy, is it consistent with the organisation's code of conduct and any overall fraud and corruption control policy?
- ☐ Does the policy state the timeframe for responding to a PID?
- ☐ Are the principles of the PID Act incorporated in the organisation's policies and procedures relating to external stakeholders, such as clients, suppliers and contractors?
- ☐ Has the organisation documented the mechanisms to protect and support disclosers?
- ☐ Is there a formal PID reporting system, such as nominated officers to receive and manage PIDs? If so:
  - ☐ are these officers adequately trained in all aspects of the PID program?
  - ☐ is this reporting system well-known and easily accessible to all employees?

- ☐ are managers given additional training in handling PIDs?
- ☐ are there sufficient designated and trained officers available to manage PIDs?

☐ Do the organisation's officers:

- ☐ clearly understand their obligations to report suspected fraud, corruption and maladministration?
- ☐ have a clear understanding of what constitutes a PID?
- ☐ know how to make a PID?
- ☐ know what to do if they receive a PID in their role as a supervisor or manager?

☐ Is the effectiveness of the support and protection mechanisms regularly monitored and reviewed?

☐ Have guidelines about acceptable behaviour for disclosers been formally established, documented and distributed?

☐ Have the support and protection mechanisms been effective (e.g. is there any evidence that disclosers have suffered reprisals in any manner)?

☐ Are the PID records periodically reviewed?

☐ Are there procedures to ensure follow-up of identified risks or deficiencies?

☐ Is the organisation's PID report linked to the organisation's risk management program?

☐ Are there programs to actively encourage an ethical work climate and an atmosphere of transparency and responsible reporting that fosters PIDs?

Chapter 6 – External reporting

The topics covered in this chapter are:

- The context of organisational reporting
- Integrity agencies
- What they do
- Integrity agencies' roles in fraud and corruption control
- Reporting policies and procedures
- Annual reporting requirements
- Best-practice target

The context of organisational reporting

Where suspicious activities are found within an organisation, appropriate action must be taken to investigate and bring any wrong-doers to account. Oversight by external integrity agencies increases the likelihood that fraud and corruption will be dealt with appropriately. However, this can only occur if the activities are brought to the attention of the external agencies. For this reason, reporting of particular suspicions and instances is a legislated requirement of each jurisdiction relevant to the type of conduct. The CC Act requires that the CEO report any suspected corrupt conduct (CC Act section 38).

This chapter outlines the obligations for organisations to report suspected fraud and corruption. It should be read in conjunction with Chapter 4, Reporting systems, and Chapter 5, Public interest disclosures.

Integrity agencies

Queensland's public sector integrity framework includes several independent statutory agencies which have complementary roles, responsibilities and powers to promote good governance, accountability and integrity.

These include:

- the CCC
- the Queensland Ombudsman (QO)
- the Queensland Audit Office (QAO)
- the Queensland Integrity Commissioner
- the Office of the Information Commissioner.

Their integrity-building activities are supplemented by the law enforcement role of the QPS.

Each of these bodies plays an important role in dealing with fraud and corruption.

The CCC receives complaints about suspected corrupt conduct and determines the most appropriate action to deal with them. The CCC has the power to investigate cases of serious or systemic corrupt conduct in the public interest or to refer the matter to the organisation for it to deal with. When it refers a complaint to a department or other agency to investigate, the CCC monitors the quality of the organisation's investigation to ensure that the outcome is reasonable and appropriate. It also assists organisations to enhance their capacity to prevent and deal with corrupt conduct. Its ambit includes state government departments including the QPS, public sector agencies and statutory bodies,

government owned corporations, universities, TAFEs, courts, prisons, tribunals and elected officials including state government politicians and local government councillors (CC Act).

Corruption includes “corrupt conduct” and “police misconduct”. Corrupt conduct is defined in the Introduction of this Guide. Police misconduct is any conduct (other than corrupt conduct) that is disgraceful, improper or unbecoming a police officer, shows unfitness to be or continue as a police officer; or does not meet the standard of conduct the community reasonably expects of a police officer. Fraud and corruption fall within both these definitions.

See <www.ccc.qld.gov.au>.

The Queensland Ombudsman reviews the actions and decisions of Queensland state government agencies, local government and some universities that may be:

- made for an improper purpose or on irrelevant grounds
- illegal or contrary to law
- unreasonable, unjust, improperly discriminatory
- based on a mistake of law or fact
- made without giving reasons, or
- simply wrong.

Some of these actions or decisions may indicate fraud or corruption.

The Ombudsman is also the oversight agency for Public Interest Disclosures under the PID Act (see Chapter 5).

See <www.ombudsman.qld.gov.au>.

The Queensland Auditor-General’s role, through the QAO, is to provide assurance to parliament on the accountability and performance of the Queensland public sector. This is achieved through the provision of independent audit services and reports tabled to the parliament on the results of those audits.

The *Auditor-General Act 2009* provides the principal legislative basis for the Auditor-General to access all government information for the purpose of performing financial and performance audits and the freedom to report findings arising from audits and for the operation of the QAO. Financial audits are conducted over every public sector entity each year. Performance audits are undertaken to assess whether agencies are achieving their objectives effectively and efficiently. Audits of non-government bodies may also be performed for the purpose of assessing how government funding has been used.

Deliberately mis-stating information about the true financial position of an agency in its Annual Report is fraud and those who do this can be prosecuted under the Criminal Code Act 1899. Equally, it is an offence for a senior officer to direct others to prepare information for publication in the annual or other statutory reports that is knowingly false or misleading, and such a direction may lead to charges of fraud, corruption or other offences.

By monitoring and reporting on compliance and other operational practices, the QAO promotes the accountability of public sector entities to the parliament and other stakeholders. The QAO’s observations and recommendations assist agencies to identify weaknesses and implement appropriate measures to address and mitigate identified fraud and corruption risks.

See <www.qao.qld.gov.au>.

The Queensland Integrity Commissioner was established by parliament to maintain and enhance the integrity of the Queensland public sector by providing advice to ministers, MPs, senior public servants and others about ethics and integrity issues, including conflicts of interest. The Commissioner is also

responsible for maintaining the Register of Lobbyists and monitoring compliance with the *Integrity Act 2009* and the Lobbyists Code of Conduct.

See <www.integrity.qld.gov.au>.

The Office of the Information Commissioner was established by the *Right to Information Act 2009* and the *Information Privacy Act 2009* to promote access to government-held information and to protect people's personal information held by the public sector. It deals with privacy complaints and makes decisions on whether an agency's privacy obligations can be waived or modified in the public interest.

See <www.oic.qld.gov.au>.

The Queensland Police Service is responsible for upholding law and order in Queensland, for detecting offenders (including fraud and corruption offenders) and bringing them to justice. Its primary legislative basis is the *Police Powers and Responsibilities Act 2000* and the *Criminal Code 1899.*

See <www.police.qld.gov.au>.

Integrity agencies' roles in fraud and corruption control

The integrity agencies offer a range of external reporting channels and advice, depending on the nature and scope of the alleged conduct. They enable the organisation's officers to report suspected fraud and corruption externally so that appropriate action can be taken.

Reporting suspected fraud or corruption and other corrupt conduct committed by an external party

Actions involving suspected fraud or corruption committed against an organisation by an external party should be reported directly to the CEO and to the QPS, and can be reported directly to the CCC. The public official (usually the CEO) of each public sector organisation has a statutory obligation to report any suspicion of corrupt conduct to the CCC.

Reporting suspected fraud, corruption and other corrupt conduct committed by employees

All cases of corrupt conduct (which includes fraud and corruption) should be brought to the notice of the public official (usually the CEO). The public official of each public sector organisation has a statutory obligation to report any suspicion of corrupt conduct to the CCC.

There are special arrangements where the corrupt conduct involves the public official/CEO. Under section 48A of the CC Act, each public sector organisation must have a policy about how a complaint that involves, or may involve, corrupt conduct by the public official/CEO will be dealt with, so that transparency and integrity in the complaint-making and resolution processes are maintained.

To assist public sector organisations, the CCC provides an outline of what such a policy should include, and a suggested template which public sector organisations may reproduce or draw on for guidance in the development of their own policy. The outline sets out a suggested structure and core elements, with some additional notes. Public sector organisations are obligated to consult with the CCC in the development of this policy.

See <www.ccc.qld.gov.au/research-and-publications/publications/ccc/48a.doc>.

There are additional reporting requirements for the QPS. Under the *Police Service Administration Act 1990*, it is the duty of all QPS officers and employees to report internal cases of misconduct to both the Commissioner of Police and the CCC. If the Commissioner of Police reasonably suspects a matter may involve police misconduct, the Commissioner is obliged to report the complaint, information or matter to the CCC.

Any individual may report suspected corrupt conduct directly to the CCC in a number of ways: in writing (mail, email, on-line form or fax) or by telephone, including anonymously, or in person.

Organisations are encouraged to report by means of the online form on the CCC website, but can also notify the CCC by letter. It is best to establish a protocol or standard format for reporting to the CCC to ensure that reported matters contain as much information as possible to help the CCC assess the complaint. (CCC *Corruption in focus*, p. 2.5).

The CCC registers all reports and assesses them to see whether they are within the Commission's jurisdiction and what action, if any, is most appropriate to deal with the allegations. The CCC may investigate the matter itself, or may refer it to the relevant department or agency subject to monitoring by the CCC. (See the CCC's publication, *Corruption in focus* and Chapter 7 of these guidelines for more details.) Alternatively, the CCC may refer any criminal activity aspects of the conduct to the QPS and the disciplinary aspects to the relevant department or agency. The person making the allegation will be notified of the outcome in due course.

Information on individual and organisation reporting obligations, and how to report, is available from the CCC in hard copy form or on the website www.ccc.qld.gov.au.

Reporting breaches of the Lobbyists Code of Conduct

Lobbying is the act of attempting to influence decisions made by officials in government. Lobbying is a normal and acceptable action by a member of a democratic society, and is an important mechanism by which governments gain information. However, a person who is paid to try to influence government decisions on behalf of a group or individual is a professional lobbyist and must be listed on the Lobbyist Register. Once registered, the lobbyist must adhere to the Lobbyists Code of Conduct. Professional lobbyists attempting to lobby public officials without being registered, or breaching the Lobbyists' Code of Conduct, can lead to perceptions of corruption and are to be reported to the Integrity Commissioner. If a lobbyist is found to have breached the Lobbyists Code of Conduct they may be de-registered and will not be permitted to continue as a lobbyist.

Any attempt to unduly influence a government decision through the offer of bribes, individual rewards or incentives is an offence and must be reported to the CEO who will decide any appropriate further reporting. (See the Integrity Commissioner's website <www.integrity.qld.gov.au>).

Reporting loss of the organisation's money or property

There are specific obligations placed on CEOs to report losses of money or property. The obligations depend on whether the loss is:

- a "material" loss
  - for local government, this is cash or equivalent of more than $500, or an asset valued at over $1000
  - for a department or statutory authority, this is cash or equivalent of more than $500, or an asset valued at over $5000
- a reportable loss, which is a loss resulting from:
  - a criminal offence, or
  - corrupt conduct of an employee, local government worker or councillor, or
  - conduct of a consultant or contractor engaged by the organisation where the conduct would be corrupt conduct if the contractor were a councillor, local government employee or local government worker, or officer of the organisation.

CEOs, accountable officers and statutory bodies must keep a written record of the details of all losses that are either material and/or reportable, and of the actions taken to remedy any weakness in the organisation's internal controls (FPMS sections 21 and 22; LG Reg 307A (1) and (2)).

Once a CEO, accountable officer or statutory body becomes aware of a loss of any of the organisation's property that may be the result of an offence under the *Criminal Code Act 1899* or another Act, the accountable officer or statutory body must notify the appropriate Minister, the QAO and the QPS (FPMS, section 21(1) and (3); LG Reg 307A (3)).

If the loss involves suspected corrupt conduct, the matter must be reported to the appropriate Minister, the QAO and the CCC (FPMS, section 21(1) and (3); Local Government Regulation 2012 section 307A (3)). The CCC then has the option of investigating the matter itself or referring it to the QPS or the organisation (see above). The following table summarises the CEO's obligations.

	Local Government	**Departments and Statutory Authorities**
Relevant legislation	LG Reg section 307A	FPMS sections 21 and 22; Schedule Dictionary for definitions
A "material loss" is:	Cash or equivalent over $500 Assets valued at over $1,000	Cash or equivalent over $500 Assets valued at over $5,000
All losses that result from a criminal offence or suspected corrupt conduct	• Must be recorded	
All material losses	• Must be recorded • Must be reported to: – the appropriate Minister – the Auditor-General	
Material losses that result from criminal offences	• Must be recorded • Must be reported to: – the appropriate Minister – the Auditor-General – QPS	
Material losses that result from suspected corrupt conduct by employees or contractors	• Must be recorded • Must be reported to: – the appropriate Minister – the Auditor-General – CCC	

Reporting complaints regarding administrative decisions

Complaints about administrative matters should be directed to the Queensland Ombudsman. The Ombudsman is not commonly involved in fraud and corruption matters, although such incidents may give rise to administrative issues in their resolution. Close liaison is maintained between the CCC and the Ombudsman to ensure that cross-jurisdictional matters are handled appropriately. Nevertheless, the Ombudsman is not an alternative complaints avenue to the CCC, and vice versa. Dissatisfaction with advice from one agency does not mean the issue falls within the jurisdiction of the other.

The Ombudsman makes recommendations to agencies to correct decisions if necessary. The organisation's reporting systems should outline the matters likely to be of concern to the Ombudsman, such as not acting on complaints, and unfair employment or tendering processes.

For more information see <www.ombudsman.qld.gov.au>.

Reporting Public Interest Disclosures

All PIDs must be reported by the organisation to the Ombudsman in accordance with specified formats. There must be adequate record keeping at all stages to enable timely and accurate reporting to the Ombudsman as mandated in the *Public Interest Disclosure Act* section 33.

The PID Act does not require organisations to report on PIDs in annual reports. However, the Department of the Premier and Cabinet (DPC) has the authority to issue specific requirements which may change from year to year. For further information check the document, *Annual Report Requirements for Queensland Government Agencies* prepared by DPC.

For more information see <www.ombudsman.qld.gov.au>.

Reporting policies and procedures

When a matter falls within the jurisdiction of more than one integrity body, the CEO of the organisation must ensure that it is reported to each one that is relevant. Organisations therefore need to develop sound reporting policies and procedures that cater for these potentially overlapping requirements — either by specific policies and procedures or through reporting mechanisms incorporated within more general arrangements covering the full scope of the organisation's reporting obligations.

The procedures for external reporting of fraud and corruption should detail the kind of conduct to be reported, and to whom, how, and when to report, and what action is to be taken by the officer within the organisation who officially receives the report. They should cater for disciplinary action if the policy and procedural requirements are not met.

Good reporting procedures will include an outline of any investigative and follow-up processes (see Chapter 7), and what the reporting person can expect to happen after they have submitted a complaint. Effective feedback is a crucial part of the communication process (see Chapters 9 and 10).

The organisation should ensure that training is provided to employees regarding external reporting and the processes around reporting obligations.

Annual reporting requirements

Annual reports are a tool for external reporting of the operation of an organisation's fraud and corruption control plan.

Specific authorised officers of a department or statutory body must certify whether, in their opinion, the annual financial statements are compliant with requirements for establishing and keeping the organisation's accounts, and present a true and fair view (in accordance with accounting standards) of the organisation's transactions for the financial year (section 42, FPMS).

The Financial Reporting Requirements (FRRs) for Queensland Government Agencies also require that a Management Certificate must be provided by the accountable officer and the CFO of the department or, in the case of a statutory body, the Chairperson and the person responsible for financial administration of the statutory body. The Certificate must state, in addition to the requirements under the *Financial Accountability Act 2009* section 62(1), that the assertions in the certificate are based on an appropriate system of internal controls and risk management processes being effective, in all material respects, with respect to financial reporting throughout the reporting period.

The *Public Sector Ethics Act 1994* section 12K makes it a requirement for CEOs of public service agencies to ensure that public officials are given access to appropriate education and training about public sector ethics. Section 12M makes it a requirement for those CEOs to include a statement about their implementation of this requirement in their annual report.

The FPMS (section 49) also directs that the requirements in the document, *Annual Report Requirements for Queensland Government Agencies* (prepared by the Department of the Premier and Cabinet) are met. These reporting requirements may change from year to year. The purpose of these changes is to improve the quality of the content of reports and financial statements, as well as integrity-related matters.

Best-practice target

(1) The organisation should have a clear understanding of the type of actions that would raise the suspicion of fraud and corruption, based on the risk identification and management processes already undertaken. (See Chapter 2: Risk management system.)

(2) The organisation should have clear policies and detailed procedures regarding the obligations for the reporting of fraud and corruption to relevant external bodies.

(3) These policies and procedures should outline how and when to report to the CCC, Ombudsman, QAO, Office of the Integrity Commissioner and the QPS.

(4) The different external reporting obligations should form part of the overall reporting arrangements developed to support the organisation's fraud and corruption control program.

Additional reading

- *Queensland Treasury Financial reporting requirements for Queensland Government Agencies*

Checklist: External reporting

The following questions are indicative only. Each organisation should develop its own checklist to reflect its specific needs and risk environment. The checklist should be re-examined and updated periodically, as part of the organisation's program of fraud and corruption control appraisal.

Legislative requirements

- ☐ Has the organisation developed a clear policy covering both mandatory and optional reporting of fraud and corruption matters to external organisations, including the:
  - ☐ CCC? (CC Act sections 38, 48A)
  - ☐ Ombudsman? (PID Act sections 33, 58)
  - ☐ QAO? (FPMS section 21 (3)
  - ☐ Integrity Commissioner?
  - ☐ Information Commissioner?
  - ☐ QPS? (FPMS section 21 (3) (c))
- ☐ Do established procedures ensure that reports of suspected corrupt conduct are brought to the attention of the CEO for transmission to external bodies? (CM Act section 38)
- ☐ Do established procedures ensure that reports of suspected corrupt conduct against the CEO are brought to the attention of the CEO or nominated officer for transmission to external bodies? (CM Act section 48A)
- ☐ Does the reporting system ensure that allegations, in addition to being reported to the CEO, are also reported to appropriate external bodies such as:
  - ☐ the CCC (possible corrupt conduct)? (CC Act sections 38, 48A)
  - ☐ the QPS (possible criminal conduct)? (FPMS section 21 (3) (c))
  - ☐ the Queensland Ombudsman (PIDs and possible maladministration)? (PID Act section 33)
- ☐ Do the external reporting policies and practices effectively address all legislative requirements and best-practice guidelines of the CCC/QAO/Ombudsman/Integrity Commissioner for reporting of corrupt conduct and other integrity matters?

Recommended Best Practice

- ☐ Are there specific arrangements or operational protocols, outlining reporting criteria and individual responsibilities for reporting?
- ☐ Are reporting requirements and options covered by the organisation's education and awareness activities?
- ☐ Are there disciplinary provisions that apply if reporting requirements are not met?
- ☐ Is there a periodic review process that systematically examines the organisation's external reporting requirements to ensure that when a change to the requirements occurs the new reporting obligations are met?

Chapter 7 – Investigation management processes

The topics covered in this chapter are:

- The catalyst for investigation
- Preliminary inquiries
- CCC involvement
- Managing the investigation process
- The organisation's response
- The investigative process
- Investigation policy
- Education and awareness
- Best-practice target

The catalyst for investigation

Possible fraud and corruption can come to the attention of the organisation through:

- the organisation's own investigations, such as data analytics or internal audits
- a report from inside the organisation
- a report or complaint from an external source such as a client, service provider or a member of the public
- an allegation in the media
- a referral from another organisation or from the CCC.

Once suspected fraud or corruption has been identified or reported, a number of processes must follow. The appropriate processes will depend on the nature and seriousness of the alleged conduct. Minor complaints are best dealt with by prompt managerial action. When dealing with serious matters where the conduct would, if proved, be a criminal offence, or provide reasonable grounds for dismissal, a full investigative response is required.

In most cases the organisation will need to manage initial receipt of the complaint, and then conduct preliminary inquiries to establish the substance of the matter to determine the most appropriate action to take. These preliminary enquiries must be limited to determining whether there is a reasonable suspicion that corrupt conduct has occurred.

If preliminary enquiries result in a reasonable suspicion that the matter may involve corrupt conduct, the CEO is bound by the *Crime and Corruption Act 2001* section 38 to report the matter to the CCC. Since fraud and corruption fall within the definition of "corrupt conduct", these matters will automatically need to be reported.

Matters involving suspected fraud or corruption committed against the organisation by an external party should also be reported directly to the QPS.

(See Chapter 6 for more information about reporting obligations.)

Preliminary inquiries

Generally preliminary enquiries should be handled by a dedicated team or a specified person within the organisation. Large organisations might have an ethics or integrity unit which would be the most appropriate area to conduct preliminary enquiries. Small organisations might have a person who takes on this role when the occasion arises.

The organisation's preliminary inquiries must be limited to determining whether there is a reasonable suspicion that corrupt conduct may have occurred, not seeking to gather information to show that the conduct complained about did occur, and there must be no enquiries by way of interviewing anyone. However, information that is already available may show that the conduct complained of could not have occurred, in which case there is no reasonable suspicion, and no requirement to report to the CCC.

Preliminary inquiries involve the consideration of any relevant information in the direct knowledge of relevant officers (such as the manager of the person complained about), or contained in the organisation's records, in deciding whether an allegation raises a reasonable suspicion of corrupt conduct. Care should be taken to ensure that information is not be taken at face value. For example, relying on timesheets or rosters to determine if there is a reasonable suspicion about an officer's conduct in work time can be misleading, as these records could have been falsified by the subject officer.

No investigation is to occur and no action is to be taken against an officer in relation to a complaint until the CCC has been notified and a response has been received about how to deal with the matter.

CCC involvement

On the basis of a reported complaint, the CCC may:

- ask the organisation to carry out further enquiries before a final assessment is made
- investigate the matter itself
- refer the matter back to the organisation for investigation, or
- investigate the matter in cooperation with the organisation – this approach may be undertaken for a variety of reasons, including if it is in the public interest, and where particular investigative powers are required.

The CCC may also choose to refer allegations involving criminal offences to the QPS.

On occasion, a complaint regarding suspected corrupt conduct may have been made directly to the CCC and the first report the organisation hears of the matter will be from the CCC.

The organisation's response

There is no single best way of dealing with a matter that the CCC has referred to an organisation for investigation. There are several valid responses, depending on the nature of the particular complaint. Of crucial importance are the procedures and investigative processes adopted by the organisation. The investigation response must reflect the nature and seriousness of the matter, and ensure that every facet of inquiry is robust enough to withstand close scrutiny. The procedures should be clearly documented. The key here is to be able to demonstrate a process that would satisfy a reasonable member of the public that the response was free from bias and the result was, on balance, fair.

The investigation process

It is imperative to have sound investigation practices. A key resource to assist organisations with this is the CCC's publication *Corruption in focus* (CCC, 2014). It gives organisations clear advice on how to deal with suspected corrupt conduct matters and recognise precisely when to refer a matter to the CCC, and explains the CCC's monitoring role. It also gives practical advice about the best way of dealing with complaints and how to conduct an investigation.

The following information is drawn from *Corruption in focus*.

Key considerations

Legality – If there is any doubt about the organisation's powers to gather information, appropriate legal advice should be sought by the organisation from Crown Law (where appropriate), or from an external legal consultant who has been appointed under approved procurement procedures.

Procedural fairness – also referred to as "natural justice". This is applies to any decision that can affect the rights, interests or expectations of individuals in a direct or immediate way, and is a safeguard for the individual whose rights or interests are being affected. It is therefore an integral element in the way complaints are dealt with.

These rules of procedural fairness require that the investigator:

- avoid bias, and
- give a fair hearing.

The investigator must remain impartial throughout the investigation. They must not have, and must not be perceived to have, any conflict of interest in relation to the complaint, or to the people, the conduct, or the policies and procedures that are the subject of the investigation.

Procedural fairness involves rigorous checking of facts, identification of issues and consideration of all relevant points of view. It benefits the investigator by revealing any issues that might expose any weakness in the investigation or areas in which the investigation is likely to be probed or attacked.

Further information on procedural fairness is provided in *Corruption in focus* Chapter 5.

Confidentiality – Appropriate confidentiality is crucial to ensure the integrity of the inquiry and to minimise the impact of the investigation. Prudent handling of materials and information minimises the risk of evidence being contaminated, possible reprisals against any discloser, prejudice against the subject officer or prejudgment of the outcomes. Confidentiality has many dimensions and may include restrictions on:

- the fact that an investigation is being conducted and who it involves
- the subject matter
- the identity of the source of the information (including the discloser)
- information collected by the investigator
- the identity of any witnesses
- any documents gathered during the course of the investigation
- discussions by witnesses about the contents of the investigation between themselves or with third parties.

Although all reasonable attempts must be made to maintain confidentiality at all times, it is not possible to promise anonymity to the person who has made the complaint or to any witnesses. At some stage their names may need to be disclosed.

Further information on confidentiality is provided in *Corruption in focus* Chapter 5.

Determining the scope and nature of any investigation

The organisation needs to be clear about what kind of investigation will be required so that this can be imparted to the investigator.

The scope should also make it very clear whether the Investigator is simply to gather information for consideration, or is required to:

- make findings about the conduct of the subject officer
- make findings about the organisation's policies and systems
- make recommendations as to the appropriate action
- recommend redress for anyone who has suffered detriment because of the conduct.

An investigation is not a consultative or advisory activity. It is driven by specific issues defined within the scope of the investigation brief. If a matter appears relevant but is not within the scope of the investigation, the Investigator should seek approval to change the scope before proceeding.

Choosing an investigator

The scope of the investigation will determine:

- powers that will be needed in order to conduct the investigation
- resources needed
- authorisations required to undertake the investigation
- outcomes required.

Powers are drawn from the legislation, guidelines or policies governing the disciplinary system applicable to the organisation, which generally set out who may conduct disciplinary investigations. The investigator is then authorised by the CEO under the powers provided by the legislation to conduct the investigation.

It is advisable to choose an investigator who has demonstrated knowledge and experience relevant to the allegations. It is therefore often a specialist internal unit, external consultant (including retired former senior officials), or senior member of staff that is given responsibility for an investigation.

Where possible, an investigation should not be conducted by anyone with direct involvement with the person or complaint being investigated. In some instances it may be appropriate to appoint the subject officer's supervisor to investigate a complaint, but not if the conduct complained of was directly or indirectly influenced by the supervisor's actions or inaction.

Care also needs to be taken to ensure that whoever is chosen to conduct the investigation has no conflict of interest or bias either for or against the subject officer. Best practice dictates that the person appointed to conduct the investigation should sign a declaration disclosing any conflict of interest and how any conflict will be managed. In larger organisations this may not present any problems. However, in smaller organisations more care needs to be taken to conduct, and be seen to conduct, an unbiased investigation. If the organisation is unable to find a suitable person within the organisation, the investigation may need to be outsourced.

Planning the investigation

A good investigation starts with careful planning and preparation, with a clear understanding of the parameters of the investigation. Planning is essential to ensure that:

- the investigation is carried out methodically and in a professional manner
- resources are allocated and used to best effect
- additional resources (including time) can be made available if required
- sources of evidence are not overlooked

- opportunities for people to remove, destroy or alter evidence are minimised.

The investigation plan should be completed before any enquiries are conducted. The plan will ensure the investigation stays focused and help to identify any potential problems before they arise.

An investigation plan also facilitates effective supervision by informing investigation managers of proposed investigative strategies and timelines in advance and during the course of an investigation (see *Corruption in focus* p. 6.7 for a sample investigation plan.)

Gathering the evidence

Evidence collected during an investigation consists of witness statements and other tangible material and intangible information. During the collection phase the investigator cannot be certain which evidence will be produced in court; therefore they must have a sound understanding of the rules of evidence, and know how to gather and protect relevant information and material so that it will stand up as evidence in a court of law.

Corruption in focus Chapter 7 summarises some key information regarding evidences.

Interviewing

All witnesses should be interviewed. Decisions will be made later about which witnesses and witness statements add value to any subsequent legal process.

Usually the complainant is the first person to be interviewed. The order of the remaining witnesses may depend on:

- the importance of their information
- the degree of their association with the subject
- their availability.

The subject of the complaint is usually interviewed last. This enables the Investigator to collect as much information as possible first, giving the interviewer a more in depth understanding of the circumstances and better able to determine the appropriate questions to ask. It also minimises the risk of evidence being tampered with or witnesses being intimidated.

Specialist training should be provided to investigators. Certification of training and investigative competency enhances the credibility of an investigator as a witness.

See *Corruption in focus* Chapter 8 for more information on interviewing.

The final report

At the completion of an investigation, the information and material must be analysed and assessed for its evidentiary value, and a report prepared. (*Corruption in focus* Chapter 9 includes a sample investigation report.)

All paperwork must be completed and filed. This work forms the organisation's formal record of inquiry, which must be held securely and be readily retrievable. All evidence must be retained until the case is fully closed, and any criminal charges or disciplinary action arising from the investigation have been finalised. This material may be subject to discovery processes or outside scrutiny by agencies such as the CCC, the Queensland Ombudsman or other representatives involved in the legal process. Retention or disposal is then done in accordance with the organisation's policies in this regard and with the *Public Records Act 2002*.

Prevention

Regardless of the final outcome, complaints and investigations can highlight particular gaps in current internal controls or practices that expose the organisation to an identifiable risk of fraud or corruption. After every investigation, an action plan or prevention response should be developed to minimise the risk of similar events in the future. The relevant employees should be included in developing these plans so they gain a sense of ownership.

The extent of the prevention response should be commensurate with the risk. A major prevention exercise does not need to be instituted when the risk is low and the consequences are minor or immaterial. Nor should there be merely a cursory examination of prevention options when an organisation identifies major risks that could have significant consequences.

Prevention initiatives are not optional. Effective risk management and internal controls are required by the FA Act section 61, the FPMS sections 4, 7, 8 and 15, and the LG Reg sections 164 and 207. Minimising opportunities for corruption and implementing effective control measures are central to good governance, minimise the costs from corrupt conduct, and contribute to the integrity of the public sector. Prevention is also a key part of upholding the ethics values set down in the PSE Act.

The scope of the investigation brief is to include a requirement by the investigator to examine and form a view about the effectiveness of the internal controls associated with the alleged conduct. The investigator is to specifically comment about these controls and make recommendations for improvement in order to assist the CEO to fulfil their obligation under the FPMS section 8 and the LG Reg section 164.

Investigation policy

The organisation's policy on dealing with investigations usually forms part of its broader disciplinary policy framework. It should take into consideration:

- who has the authority to initiate the investigation
- the primacy of natural justice in the process
- confidentiality of information
- determining the extent of the investigation
- the conduct of interviews (with all parties and in different formats)
- attendance at disciplinary hearings
- progress reports
- investigation report
- overview by an organisation or nominated senior management.

The policy and related procedures and guidelines should be reviewed regularly (at least every three years).

Education and awareness

Education and awareness programs should be provided to inform employees about what to expect if they become involved in an investigation. This can assist with minimising the adverse impacts of an investigation. This knowledge is particularly important for supervisors and managers.

Strategies to help public sector managers and supervisors manage the impact of an investigation are provided in Chapter 5 of *Corruption in focus.* This is particularly helpful for key personnel, including managers and supervisors, faced with the realities of a potentially disruptive situation.

Best-practice target

(1) The organisation should have an investigation policy that emphasises the organisation's commitment to legality, procedural fairness and confidentiality.

(2) The organisation should have robust investigation procedures that provide suitable direction in determining the best-practice approach for any investigation, based on the nature and seriousness of the matters to be investigated, and that outline the roles and responsibilities of management and investigators.

(3) The policy and procedures should be communicated throughout the organisation.

(4) Well-trained and experienced investigators, with specialist training in fraud and corruption investigative techniques, should be included in more complex investigations.

(5) The investigative standards should be at least as stringent as those outlined in the CCC publication *Corruption in focus*.

(6) Every investigation process should include the development of a prevention action plan to minimise the risk of similar events in the future.

(7) Every step of the process from receipt of report to the conclusion and closure of the matter should be carefully documented.

Additional readings

- CCC 2014, *Corruption in focus.*

Checklist: Investigations management processes

The following questions are indicative only. Each organisation should develop its own checklist to reflect its specific needs and risk environment. The checklist should be re-examined and updated periodically, as part of the organisation's program of fraud and corruption control appraisal.

Recommended Best Practice

- ☐ Does the organisation have policies and procedures to address the investigation process?
  If so, do they cover:
  - ☐ powers to investigate as per the relevant Act?
  - ☐ authorisation by the CEO to investigate?
  - ☐ ability of the CEO to delegate powers?
  - ☐ authority to initiate investigations?
  - ☐ requirements of natural justice/procedural fairness?
  - ☐ scope or extent of the investigation?
  - ☐ confidentiality matters?
  - ☐ conducting interviews?
  - ☐ security of evidentiary materials?
  - ☐ attendance at disciplinary hearings?
  - ☐ progress or status reports and the investigation report?
  - ☐ overview by any organisational integrity unit and/or designated executive?
- ☐ Do preliminary complaints-handling arrangements minimise the risk of prejudicial actions or potential hindrances to any further investigation?
- ☐ Are trained internal officers, or suitably qualified external investigators, responsible for conducting investigations?

Are investigators selected based on:

- ☐ their independence and freedom from any conflict?
- ☐ their demonstrated knowledge and experience in the area relevant to the allegations?

- ☐ Are investigators appropriately and properly authorised under legislation and by policy to conduct the investigation?
- ☐ Are there clear procedures as to when and how investigators are briefed and instructed to proceed in any given fraud, corruption or corrupt conduct situation?
- ☐ Is particular attention given to natural justice, procedural rigour, security and relevant expertise in taking and securing evidence?
- ☐ Are the organisation's investigative guidelines reviewed regularly (e.g. at least every three years)?
- ☐ Are there adequate reporting systems to keep management and any other relevant parties (e.g. the CCC) informed of the ongoing status of investigations?
- ☐ Does every investigation process include the development of a prevention action plan to minimise the risk of similar events in the future?
- ☐ Are responsibilities clearly assigned and relevant systems developed to ensure that full and complete records are maintained of all potential fraud and corruption investigations?
- ☐ Are records of all reports of fraud and corruption investigations held securely, with minimal opportunities for tampering or unauthorised access or removal?

- ☐ Are there clear guidelines about the ongoing storage of investigation material after the matter has been closed?
- ☐ Is there a secure location, which ensures no unauthorised access, that is used to store investigation material until it can be legally and appropriately disposed of?
- ☐ Are there appropriate education and awareness programs for employees and management about the nature and impact of investigations?

Chapter 8 – Code of conduct

The topics covered in this chapter are:

- The role of a code of conduct
- The legislative framework
- Public Service agencies' code of conduct
- Public sector entities' codes of conduct
- Establishing and maintaining commitment to the code
- Best-practice target

The role of a code of conduct

Fraud and corruption is a departure from the expected standards of behaviour for public officers.

A code of conduct can help develop the expectations and standards of behaviour within an organisation, consistent with the public sector ethics principles and values. It reflects an organisation's values and philosophy, and provides the framework within which employees perform their duties. It also provides an "ethical roadmap" for employees by documenting and supplying guidance about minimum standards of expected behaviour. Effective codes provide employees with aspirational goals and boundaries to encourage ethical behaviour. They anticipate likely situations or questions that employees might face, and provide clear information as to how the organisation expects its employees to respond.

Just as importantly, an organisation's code of conduct provides benchmarks that clearly state the types of behaviours the organisation considers unacceptable. The code encapsulates the organisation's policies and procedures, the breach of which may be grounds for disciplinary action.

The legislative framework

The *Public Sector Ethics Act 1994* (PSE Act) sets the legislative basis for ethics principles and values, codes of conduct and disciplinary action in the public sector.

Having a code of conduct is mandatory for public service agencies and public sector entities as defined in the PSE Act. Codes are to provide standards for conduct that are consistent with the four public sector ethics principles set out in the PSE Act (section 4(2)):

- integrity and impartiality
- promoting the public good
- commitment to the system of government
- accountability and transparency.

The CEO must ensure that all officers have ready access to a copy of the code and is responsible for ensuring that the organisation's officials are aware of their rights and obligations in relation to any contravention of the code of conduct (PSE Act, section 12K and section 21).

It is a condition of employment for all public officials that they will comply with the standards of conduct stated in the code of conduct for their organisation (PSE Act sections 12H, 18), and the policies which underlie it.

It is important for both agencies and entities to make it clear that disciplinary action can be taken for a breach of the organisation's code of conduct or any official policy. Disciplinary action in relation to codes of conduct is to be dealt with under the relevant Act or regulation (PSE Act section 24):

- for the public service, under the *Public Service Act 2008* (PS Act)
- for local government, under the *Local Government Act 2009* (LG Act) or *City of Brisbane Act 2010*
- for all other public officers, under their organisation's disciplinary regulations or processes.

It is important that all public sector organisations have in place a clear and fair process for investigating, deciding and appropriately managing any allegations of corrupt conduct of which they become aware. It is equally important that all employees understand this process and recognise that it will be followed in every instance.

Action should be taken without delay once there is a reasonable suspicion that corrupt conduct has occurred. The value of a code as a deterrent to wrongdoing depends substantially on the perception that breaches of the code are taken seriously and acted on, and that there are demonstrable consequences for breaching the code commensurate with the nature of the breach.

A code of conduct alone will not guarantee an honest and corruption-free organisation. However, with proper education and leadership it can promote integrity and encourage ethical behaviour, which in turn strengthens the organisation's resistance to fraud and corruption.

Public Service agencies' code of conduct

Public Service agencies are defined in the schedule to the PSE Act as: a department, a TAFE institute, the administrative office of a court or tribunal, or any other entity that is prescribed under a regulation to be an agency.

These agencies are bound by the *Code of Conduct for the Queensland Public Service* (the Code). The Code applies to all Queensland public service agency employees whether permanent, temporary, full-time, part-time or casual, and all volunteers, students, contractors and consultants who work in any capacity for a Queensland public service agency (PSE Act section 11).

Who is responsible

The Public Service Commission has oversight responsibility for the Code. This oversight responsibility includes administering the Code and reviewing it regularly.

Training

The CEO of the agency is required to ensure that all employees are given access to appropriate education and training about public sector ethics at induction and at regular intervals during their employment (PSE Act section 12K). This is to include:

- the operation of the PSE Act
- the application of ethics principles and obligations to the public officers
- the contents of the code of conduct
- the rights and obligations of the officials in relation to contraventions of the code.

Reporting

The agency's annual report must include a statement about:

- the implementation of the code of conduct

- actions taken to ensure that employees were given access to training at induction and at regular intervals about public sector ethics and code of conduct, and actions taken to ensure that the administrative procedures and management practices have proper regard to the ethics principles and values, the code of conduct and any standard of practice applying to the agency (PSE Act section 12M).

Further information can be obtained from the PSC <www.psc.qld.gov.au>.

Public sector entities' codes of conduct

Public sector entities are defined in the schedule to the PSE Act as: the parliamentary service, local governments including Brisbane City Council, universities, colleges, entities established under an Act, or under State or local government authorisation for a public State or local government purpose, and entities established under a regulation.

Entities must have a code of conduct which can be either the *Code of Conduct for the Queensland Public Service* or one they develop themselves.

If the entity chooses to develop its own code of conduct, that code must be consistent with the four ethics principles in the PSE Act (PSE Act section 13), current legislation including the entity's own statute, the CC Act and the PID Act.

Who is responsible

Under the PSE Act, the CEO is responsible for ensuring that a code of conduct is developed and maintained for the entity. The CEO has several statutory obligations and must consult with all relevant parties, have the code approved by the responsible authority, and ensure that the code is accessible by all entity officers (PSE Act, sections 15–17, 19).

Developing a code of conduct

An entity should always look at developing and adopting a code of conduct as far more than merely completing a compliance activity, and should ensure extensive consultation with stakeholders (despite the time and patience this requires). To approach the matter as merely an administrative obligation misses an opportunity to communicate to staff the importance of their key role in working for and on behalf of their community (i.e. the people of Queensland). A failure to establish the principles of working with integrity and ethics and in the public interest carries the risk of potentially greater long-term losses through fraud and corruption, and the associated costs of investigations and possible disciplinary action.

A code of conduct must be practical. Managers and employees must be able to understand and communicate its requirements and be able to readily identify the relevant standards of conduct that apply to them.

In addition to the provisions covering the ethics principles outlined in the PSE Act, the code of conduct may contain broader guidelines and procedures that are relevant to fraud and corruption control.

The code of conduct should be reviewed regularly, at least every two years, to ensure it is still relevant.

Training

The CEO is required to ensure that all employees are given access to appropriate education and training about public sector ethics, including the contents of the entity's code of conduct (PSE Act section 21). This is to include:

- the operation of the PSE Act
- the application of ethics principles and obligations to the public officials

- the contents of the entity's approved code of conduct
- the rights and obligations of the officials in relation to contraventions of the approved code of conduct.

Reporting

Public sector entities that nominate to adopt the *Code of Conduct for the Queensland Public Service* by regulation are considered public service agencies for the purposes of the PSE Act and should follow the reporting requirements for public services agencies.

For all other public sector entities, the entity's annual report must include a statement about:

- the preparation of a code of conduct
- actions taken to ensure that employees were given access to training about public sector ethics and the organisation's code of conduct, and
- actions taken to ensure that the administrative procedures and management practices have proper regard to the ethics principles and values, and the code of conduct applying to the entity (PSE Act section 23).

Establishing and maintaining commitment to the code

Introducing a new or updated code of conduct involves setting the ethical compass and defining the corporate culture, and this may involve substantial change. Introducing change usually takes time for discussion and consultation, communication and understanding, assimilation, acceptance, and attitudinal change.

Maintaining employee and organisational commitment and promoting the values of the code can also present great challenges. Invest time in communicating and implementing the code.

The code should be supported by complementary policies, procedures and standards covering all reasonable operational and behavioural issues. This will provide further guidance regarding what is expected of employees.

Entities not covered by the PS Act or LG Act should have their own discipline policy and procedure that make it clear that disciplinary action can be taken for a breach of the organisation's code of conduct or any other official policy.

(See Chapter 9 for more information about organisational culture change and about education and training.)

Most importantly, successful assimilation and acceptance of the code is best brought about through the actions and words of the supervisors and managers. When staff see their supervisors and managers abiding by the code and regularly discussing how the code applies within each work area, they are more likely to willingly follow the code.

Best-practice target

(1) The organisation must have a code of conduct dealing with ethical conduct.

(2) The code should be supported by complementary policies, procedures and standards covering all reasonable operational and behavioural issues.

(3) The code should be reviewed on a regular basis to ensure its continued relevance.

(4) Employees should be encouraged to participate in the development and regular review of the code of conduct in order to foster a greater sense of ownership and commitment.

(5) The code should clarify behavioural expectations and encourage the adoption of ethical behaviour that will assist with building a corruption-resistant culture.

(6) Organisations not covered by the PS Act or LG Act should have their own discipline policy and procedure that make it clear that disciplinary action can be taken for a breach of the organisation's code of conduct or any other official policy.

(7) To maintain employees and organisational commitment and to reinforce the principles embodied in the code, the organisation must provide staff at all levels with ethics training at induction and at regular intervals during their employment, and should implement a variety of extension and awareness programs, including periodic refresher and/or employees development programs.

(8) To achieve assimilation and acceptance of the code and the willing compliance of staff, supervisors and managers need to abide by the code and regularly discuss how the code applies within each work area.

Additional readings

- *The Code of Conduct for the Queensland Public Service*.

Checklist: Code of conduct

The following questions are indicative only. Each organisation should develop its own checklist to reflect its specific needs and particular risk environment. The checklist should be re-examined and updated periodically, as part of the organisation's program of fraud and corruption control appraisal.

Legislative requirements

- ☐ For public sector entities not bound by the *Code of Conduct for the Queensland Public Service:*
  - ☐ Does the organisation have a formal code of conduct? (PSE Act section 15)
  - ☐ Is that code consistent with the principles of the PSE Act and other relevant legislation? (PSE Act section 10(2))
  - ☐ Was that code developed following a comprehensive process of consultation with professional bodies and/or industrial organisations? (PSE Act section 16(2))
  - ☐ Was that code approved by the appropriate authority? (PSE Act section 17)
  - ☐ Does the entity's annual report include a statement about the preparation of that code of conduct? (PSE Act section 23)
- ☐ Are all employees and external parties (for example, customers, contractors) able to access the organisation's code of conduct? (PSE Act sections 12I, 12J, 19 and 20)
- ☐ Does the organisation's annual report include details of actions taken to ensure that employees were given access to training about public sector ethics and the organisation's code of conduct, and actions taken to ensure that the administrative procedures and management practices have proper regard to the ethics principles and values, and the code of conduct applying to the entity? (PSE Act section 12M(2) and section 23)
- ☐ Are there wide-ranging training and awareness strategies covering the code of conduct? (PSE Act section 12K and section 21)

Recommended Best Practice

- ☐ Do the code of conduct and related policies clearly outline that the organisation expects the highest ethical standards and is committed to preventing fraud and corruption?
- ☐ Does the code of conduct provide clarity around appropriate behaviour in situations that may provide opportunities for fraud and corruption to occur?
- ☐ Does the code refer to other relevant policies and resources to assist with preventing fraud and corruption?
- ☐ Do contracts with external parties (e.g. contractors) clearly state that their employees are required to uphold the organisation's code of conduct?
- ☐ Do the disciplinary policies and standards within the code complement the organisation's fraud and corruption control program and associated policies and procedures?
- ☐ Have all organisational roles and responsibilities associated with the code of conduct been clearly defined?
- ☐ Are these responsibilities properly understood and accepted by those involved?
- ☐ Is the code, and any supporting resources, reviewed periodically?

Chapter 9 – Organisational culture change program

> Official policies specify what management want to happen. Corporate culture determines what actually happens, and which rules are obeyed, bent or ignored.
>
> (Committee of Sponsoring Organisations for the Treadway Commission, 1992)

The topics covered in this chapter are:

- Why organisational culture change matters
- How to change organisational culture
- Monitoring progress
- Best-practice target

Why organisational culture change matters

Being an organisation that is truly free of fraud and corruption is an ideal worth striving for. This requires a workforce of employees who are fraud aware and fraud resistant. While you may conduct pre-employment screening of applicants, once a person is employed and working in the organisation their integrity will be influenced by what they find within your organisation. Similarly, your organisation may generally be ethical, but that will not prevent fraud from external sources or from individuals who resist that culture. Hence it is important to have a culture of integrity that is resistant to fraud and corruption within your organisation.

To maintain an ethical organisational culture requires constant work. An integrated organisational culture change program will ensure a well-informed workforce with a greater capacity to recognise and respond to the risks of fraud and corruption. The end result will be an organisation with a strong ethical corporate culture that is better equipped to detect and prevent wrongdoing.

How to change organisational culture

Creating an environment that resists fraud and corruption and rewards integrity requires a range of strategies.

The organisational change process can be grouped into three sets of activities:

- Educating and training regarding ethics and standards
- Setting ethical standards
- Enforcing ethical standards.

These are not to be executed in a linear process but should occur concurrently.

Setting standards

Every organisation sets standards to achieve a range of outcomes. Documenting and advertising these standards demonstrates to its stakeholders that the organisation has high performance expectations of itself and its staff and that it can be held accountable for these. Performance standards are documented and advertised through key documents such as mission statements, strategic plans, organisation-wide policies and procedures, standards, performance reviews, discipline processes and, critically, a code of conduct. An ethical culture should be embedded in performance standards.

Standards are also set through the attitudes espoused and behaviours demonstrated by those at the top of the organisation. Management's commitment to the program sets the tone, with senior executives leading by example and participating in the program. The involvement of management is a key factor in the success of culture change programs. If the CEO or senior managers regularly disregard the organisation's rules or do not respond to suspected wrongdoing, they cannot reasonably expect others to uphold the rules.

Enforcing the standards

This starts with regular monitoring to identify breaches. Good internal controls, especially complaint management systems, will have record-keeping processes built into them to assist with this. When a breach is found, subject to the CCC's requirements explained in Chapter 7, take action as quickly as possible. Start with an effective investigation, prior to initiating the appropriate actions in relation to anyone found to be at fault. Commit to continual improvement by feeding back lessons learned and preventative actions taken into the internal controls and the organisational change process to reduce the likelihood of a recurrence.

Enforce all anti-corruption messages fairly and fearlessly. How the organisation reacts to suspected fraud or corruption is a vital factor in the success of your culture change program. Actions speak louder than policies and procedures. If the messages are not upheld by appropriate actions at the crucial moment, much of your effort in changing attitudes and behaviours will be wasted.

Educating and training

Culture change is largely dependent on providing sufficient information and education.

Start by planning a program of communication. Include a variety of messages and mechanisms and be sure that you engage with all of your employees regardless of how long they have been within the organisation, their seniority or their role. For example, use inductions for new starters, in-depth training for specific roles that are assessed as having greater inherent risks, and reminder mechanisms like newsletters for existing employees.

Take a "job life-cycle" approach to communicating with your staff about the issue of fraud and corruption. This includes engagement during:

- Recruitment and selection processes – ensure job advertisements, key selection criteria and promotional materials carry essential information about the values and ethical standards of the organisation to prospective employees.
- Induction – make certain that new officers understand their obligations by providing suitably structured induction programs. Induction training is an opportunity to provide all new personnel with first-hand notice of the organisation's attitude towards fraud and corruption.
- Ongoing employment – as a minimum, the CEO is required to ensure that all employees are given access to appropriate education and training about public sector ethics (PSE Act section 12K and section 21). This is to include:
  - the operation of the PSE Act, and
  - the application of ethics principles and obligations to the public officials; and
  - the contents of the code of conduct, and
  - the rights and obligations of the officials in relation to contraventions of the code of conduct.

The content and time allowed for any training session will depend on the audience and the size and function of the organisation. Induction in a small organisation may involve a one-on-one discussion between a manager and a new employee; larger organisations may offer a series of information sessions over a period of time.

Provide broad programs for all staff that foster an ethical organisational culture. Include training in the detection, identification and prevention of fraud and corruption.

Provide regular targeted education including specialist and specific training for high-risk functions and for different staff groups such as those responsible for audit, purchasing, financial functions or investigations.

It is acknowledged that larger, geographically dispersed and remote organisations face particular challenges to ensure that all staff receive the same quality training. However, corrupt conduct can inflict significant harm to your organisation so ensure that quality training is implemented.

Table 9.1 lists a range of programs to consider for different staff groups.

Awareness of ethical principles and ethical decision-making skills are essential elements of fraud and corruption control. Staff development programs should build on the code of conduct and include relevant scenarios or case studies that encourage participation and link the training to everyday work situations.

The following tips specific to training in ethics may be helpful:

- Ensure that participants sign an attendance sheet at the beginning and at the end of the session. It is important to be able to establish that the organisation provided comprehensive training, and which staff were there for the entire session.
- Consider an opening address by the CEO or a senior executive – this will communicate to attendees the seriousness being placed on the training.
- Always consider the profile of your audience and seek innovative training mechanisms to ensure the training is understood.
- Take a positive approach and outline the benefits of an integrity regime.
- Avoid any implication that participants are unethical.
- Use case studies to illustrate points and generate discussion.
- Encourage participation.
- Use a variety of visual aids.
- Ensure that participants acknowledge in writing the receipt of any policy or code of conduct.
- Use evaluation sheets to provide feedback and drive program improvement.

Table 9.1: Sample Education and Training program

Audience:	**Message:**	**Mechanism**	**Frequency:**	**Supported by**
Job applicants	Organisation's stance on fraud and corruption Code of conduct	Material in position descriptions and applicants' packs	On application	Links to code of conduct on website
New starters including temps, volunteers and contractors	Organisation's values, policies, code of conduct; reporting arrangements, PIDs How to respond to suspicions of fraud and corruption	Induction sessions NB: Senior managers should be involved Need written acknowledgment of receipt of policies and procedures	In first week of employment	Policies and procedures Orientation manual Promotional brochures Intranet Self-tutoring guides
Senior managers Board members Elected officials	Risk areas identified in risk assessment Importance of modelling Case studies and techniques to further develop ethical decision-making skills Code of conduct	In-house sessions External providers including registered training providers and accredited courses Mentoring Professional development courses Tertiary education	On appointment When policies systems or legislation change If fraud, corruption or corrupt conduct occurs	Risk management process Policies and procedures Job ads and position descriptions Performance reviews Required as part of professional development or employment contract Consultation
All supervisors	How to deal with complaints received or fraud detected Handling PIDs	In-house sessions CCC, Ombudsman External providers including registered training providers and accredited courses Mentoring	Every two years When policies, systems or legislation change	Policies and procedures CCC brochures PID guides
All officers including elected officials	Refresher on code of conduct and PIDs Any changes to policies etc. in last year Refresher on ethical decision-making skills Fraud and corruption	In-house sessions External providers Professional development courses Staff meetings	Every year online When policies, systems or legislation change If fraud, corruption or corrupt conduct occurs	Risk management process Policies and procedures Performance reviews Articles in newsletters and on intranet Posters and brochures
Employees who work in high-risk functional areas identified in the organisation risk assessment	Policies and procedures Internal controls	Supervision In-house sessions External providers Self-tutoring Professional development courses Staff meetings	Every year When policies, systems or legislation change If fraud, corruption or corrupt conduct occurs	Risk assessments Policies and procedures Performance reviews

Officers responsible for detection, investigation and prevention: Internal audit Corporate governance HR, Legal	Policy development Industrial relations Human resources Evidence collection Investigation techniques Witness statements Corporate governance Risk management	Registered training providers of accredited courses Programs sponsored by professional bodies Tertiary education	Predetermine at recruitment and selection On appointment When policies, systems or legislation change When risks or fraud identified	Prerequisite qualification Mandatory as part of professional development

Constantly reinforce the messages

Apply reinforcement techniques that help institutionalise ethics, so the effects of the training remain. Focus on a range of fraud and corruption issues and use all reasonable communication means to ensure that control and prevention principles remain always at the forefront of employees' minds. Here are some suggestions:

- Implement a communication plan to promote the organisation's values and reinforce the messages provided by the ethical development programs. (See Chapter 10 for more about communication plans.) Consider:
  - organisation publications (including the organisation's annual report)
  - simple policy statements or policy briefs on at-risk areas, broadcast by email
  - material in the organisation's internal newsletters
  - regular updating of relevant information on the organisation's intranet
  - flyers, brochures and posters
  - screensavers and logon notices
  - reports on the outcomes of investigations (where appropriate).
- Find innovative ways of delivering the organisation's integrity-building messages. Search for new training products and delivery methods. Talk to other organisations to see what has worked for them. Use both formal and informal linkages to share information (such as the Corruption Prevention Network Queensland and Transparency International). The CCC has a range of material on its website <www.ccc.qld.gov.au> with links to other resources.
- Use real-life examples and situations that personalise the issues.
- Engage in "ethics conversations" and "hypotheticals", including fraud examples. Small groups and team meetings are perfect places for conversations that provide immediacy and relevance, and can be more effective than giving a lecture.
- Reward and recognise ethical behaviour. Take time to congratulate officers for a job well done or for their vigilance in detecting fraud and corruption. Focus on the positive steps the organisation has taken to minimise risk.
- After any investigation, develop an action plan or prevention response to minimise the risk of similar events in the future. Always involve the relevant employees in developing these plans so they gain a sense of ownership.

Monitoring progress

Informed employees who can recognise and deal with fraud and corruption are your best line of defence against serious fraud or corrupt activities occurring in your organisation. Well informed employees can also help to improve your organisation by identifying areas where there is reduced performance or unnecessarily expensive activities. These situations may also harbour corrupt conduct.

Conversely, failure of internal controls can indicate a failure of the organisation's culture change program. Reviewing the causes of internal control breakdowns due to human error or deliberate action, will give insights into the overall success of fraud and corruption control endeavours, and of an organisation's culture change program.

Where breaches of the internal controls are detected it will be important to review these using a multi-layered approach, considering:

- Were the initial and ongoing modes and content of communication faulty or misdirected?
- Were the designs ineffective or subject to redundancy due to redesigned systems?
- Were the key staff:
  - improperly trained
  - not supervised correctly
  - subject to negative sub-cultures working against the integrity endeavours
  - negligent or lazy?

The cause of failure to fully realise culture change may arise from any one, or a combination of, factors in the above list. Additionally, the causes for a breakdown in your attempts to change your organisation's culture may come from issues that are not on this list.

The important thing is to ensure you have reliable monitoring processes in place that will gather information from a range of sources and in a variety of ways over time.

Consider staff surveys to seek feedback on fraud awareness, employees' attitudes, and the quality of control supervision and monitoring.

The Public Service Commission's annual Working for Queensland survey can also provide some useful information regarding the workplace culture.

Best-practice target

(1) Set and document the expected minimum standards of behaviour through mission statements, strategic plans, the code of conduct, organisation-wide policies and procedures; and standards, performance reviews and discipline processes.

(2) Ensure that senior executives and management set the tone through their attitudes and behaviours, leading by example and participating in the program.

(3) Reinforce the standards through the use of good internal controls, and by monitoring to identify breaches.

(4) Act as quickly as possible when a breach is found, starting with an effective investigation, initiating the appropriate actions in relation to anyone found to be at fault, and using lessons learned to continually improve the internal controls and the organisational change process to reduce the likelihood of a recurrence.

(5) The organisation should have an effective communication, education and training program that brings fraud and corruption control to the attention of all officers.

(6) A series of different programs should be developed to suit different groups or operational cultures within the organisation. These should take a variety of formats and be placed in different contexts

including considerations such as regional, educational, language and literacy differences to be most effective.

(7) Specialist training in fraud awareness should be provided for groups such as investigators, and those performing identified high-risk functions.

(8) Complementary best-practice guides should be developed for particular activities (e.g. complaints management, procurement, internet use). These may assist in identifying potential improvements to operational practices and control arrangements.

(9) Systems should be in operation to monitor and evaluate education and training programs.

(10) The organisation should regularly assess its culture through a range of monitoring activities.

Additional readings

- CCC Advisory series provides information about the corruption risks associated with a range of topics, and strategies to prevent corruption:
    - Post separation employment
    - Social media and the public officer
    - Use of official resources
    - Conflciting commitments
    - Disposal of assets
    - Lobbying
    - Gifts and benefits
    - Management of public records
    - Information security and handling
    - Procurement and contract management
    - Sponsorship management

  <www.ccc.qld.gov.au/corruption-prevention/corruption-prevention-advisories>
- *Giving Voice to Values*, Yale University Press, 2012
- *Educating for Values-Driven Leadership: Giving Voice To Values Across the Curriculum,* The United Nations Principles for Responsible Management Education Book Collection, 2013 (ed: Mary C. Gentile)

Checklist: Organisational culture change program

The following questions are indicative only. Each organisation should develop its own checklist to reflect its specific needs and risk environment. The checklist should be re-examined and updated periodically, as part of the organisation's program of fraud and corruption control appraisal.

Legislative requirements

- ☐ Is ethical decision-making training provided at induction and at regular intervals? (PSE Act sections 12K, 21)
- ☐ Is information on provision of ethics training included in the annual report? (PSE Act sections 12M(2) and 23)

Recommended Best Practice

- ☐ Does the organisation's induction program:
  - ☐ address fraud and corruption issues?
  - ☐ include a statement from the CEO stating the organisation's attitude to fraud and corruption?
  - ☐ cover relevant legislation?
  - ☐ include details about key integrity policies and procedures such as:
    - dealing with conflicts of interest
    - gifts and benefits
    - undertaking secondary or external employment
    - purchasing and tendering
    - contract management
    - sponsorship management
    - reporting corrupt conduct
    - using official resources
    - disposing of scrap and low-value assets
    - using corporate credit cards
    - using Internet and email
    - electronic and information fraud
    - managing public records
    - handling confidential information
- ☐ Does the organisation have a structured education and training program to assist employees recognise, detect and prevent fraud and corruption?
- ☐ Is there an ongoing education and training program to address:
  - ☐ specific needs as they arise?
  - ☐ specific organisational functions (e.g. audit, investigations, PIDs)?
- ☐ Does the program take advantage of a variety of communication channels?
- ☐ Is the program evaluated regularly to determine its effectiveness?
  - ☐ If not, will it be evaluated in the future?
  - ☐ If so, have the results of the evaluations been acted upon?
- ☐ Are ethical considerations included in staff performance reviews?

Chapter 10 – Client and community awareness program

The topics covered in this chapter are:

- Why client and community awareness matters
- Relevant legislation
- How to create client and community awareness
- Developing a communication plan
- Providing clear guidelines to external service providers
- Monitoring the outcomes
- Best-practice target

Why client and community awareness matters

The community in general and clients in particular are key stakeholders and government is responsible to them. The Australian Standard for Fraud and Corruption Control states that an entity's commitment to its Fraud and Corruption Control Plan (Plan) should be communicated to all external stakeholders. (*AS 8001:2008*, p. 20)

To maintain public trust, the community must be confident that organisations and their officers behave ethically.

Some major benefits that come from good communication of the organisation's values and practices include:

- forestalling potentially unacceptable practices
- increasing the likelihood of detecting suspected fraud and corruption
- increasing service standards and satisfaction among all stakeholders
- improving the organisation's standing within the community.

Emphasising that the organisation is committed to probity and will not tolerate fraud and corruption raises morale and productivity inside the organisation and improves the commitment of staff to achieve higher standards of performance overall.

Client and community awareness means a wide-ranging knowledge and understanding of the organisation's standards of corporate and employee behaviour, including everything from policies to codes of conduct.

Your clients should be aware that it is not appropriate to give gifts, rewards or other "incentives" to staff, and that unethical dealings of any kind will not be tolerated. Clients and the community need to know that the organisation welcomes reporting of any corrupt conduct.

Such awareness of the organisation's stance on fraud and corruption does not happen automatically — effective communication programs are needed.

Better informed people are better positioned to recognise and report untoward situations. By fostering transparency and drawing attention to acceptable policies and practices, an organisation is more likely to hear about inappropriate practices from clients and other members of the community.

It is significant that the KPMG Australia and New Zealand *Fraud and Misconduct Survey* of 2010 found that in 25 per cent of cases the largest single fraud in each organisation was reported by an external

party (KPMG 2011, p. 12); however, by 2013 notifications by external parties had dropped to 10 per cent (KPMG Forensic – *Survey of fraud, bribery and corruption*, 2013, p. 28). Clearly, your organisation's best form of defence is through a combination of strong and functional internal controls, and high levels of fraud awareness in your workforce.

While awareness programs work to inform stakeholders, they also send effective messages to potential wrongdoers. Knowing about the organisation's control measures and penalties for fraud or corruption may deter corrupt behaviour or discourage people who are considering bribery or other forms of undue influence when dealing with a public official.

Good communication is significant in developing and maintaining core values, and in any behavioural change process. The process normally involves several steps:

- The organisation creates awareness of the desired behaviour through suitable communications (including education and marketing).
- The organisation fosters attitudinal change through communication that demonstrates personal, organisational or community benefits to the target audience.
- The target audiences begin to deliver behaviour change.
- The organisation maintains communication, assesses the environment in which the messages are being sent, works to maintain the behavioural change, and adjusts the messages and/or the method of delivery as necessary.

Relevant legislation

The Right to Information Act 2009 (RTI Act) aims to make information in the government's possession available to the community, while still providing appropriate protection for individual privacy. The RTI Act states that departmental policies and procedures should generally be available to the public on the basis that government information is a public resource and openness in government enhances accountability.

This mechanism provides for organisational transparency. It allows people external to the organisation the opportunity to compare their experience of the organisation against its policies. Where there is a departure between the service and the policy this provides an opportunity to ensure accountability for the level of service provided by the organisation.
In this way the organisation can be informed about employee actions which may represent fraud or corrupt conduct.

How to create client and community awareness

Developing strategies to create good awareness requires an understanding of the various stakeholders' communication needs, perceptions and constraints. It involves effective promotion of the organisation's views and attitudes while providing avenues for dialogue and feedback. It involves good communication, which will help to ensure that any fraud and corruption prevention measures are focused on clients' needs and expectations and on achieving outcomes.

Communication techniques for creating awareness may range from general communication practices used across the public sector to targeted campaigns to meet specific needs, such as particular client groups or higher-risk functions. Organisations with corporate communication units can develop independent communication plans and awareness strategies using their internal resources. Organisations can make the most of their facilities by working together, sharing ideas and materials, or using available CCC materials and other resources. A collaborative approach is particularly useful for smaller organisations or those that are geographically dispersed because it maximises use of resources and, depending on the messages, can provide synergies for other activities.

A carefully developed communication plan will help to focus on what the organisation wants to achieve and the right strategies and tools for the purpose.

It will ensure that:

- correct messages are conveyed to the right audiences
- materials are client-focused (or target-oriented)
- materials are properly disseminated and easily accessible
- messages are delivered that convey a consistent approach
- messages are delivered in a timely fashion, and in a variety of formats to suit the different target audiences.

Organisation communication objectives need to consider both the internal and the external environment when dealing with fraud and corruption. For example, the risks of fraud and corruption will be lowered by a change in the external environment where potential clients, suppliers and contractors, observe honest and ethical business practices and there is sufficient awareness of standards and practices for people to recognise and report unacceptable behaviour.

Strategic communication can achieve these goals through a combination of public awareness, attitudinal change and behavioural change.

Developing a communication plan

A well-targeted communication and awareness plan usually contains the following.

Statement of objectives

- What outcome you wish to achieve through your awareness strategies, e.g. change attitudes or behaviours; enhance the organisation's standing.

The target audience

- Who should be receiving/reading/using this information.
- Who is likely to have an interest in the topic.
- Who are the different groups you want to communicate with.

Key messages

- What significant things you want all of your target groups to know.
- What you want to say to each particular group.

Communication methods

- What you plan to do to make sure you get your messages across.
- The particular needs, perceptions and constraints of each target audience group.
- The strategies you are proposing for the target audience.
- Other events or activities to help communicate with the target audiences.
- How often to communicate.

Required resources/budget

- What budget has been allocated to cover the costs of the communication program.
- How realistic the budget is for what you hope to achieve.

Key issues

- Constraints or other issues that affect the plan (e.g. sensitivities, budget, opportunities).

Evaluation methodologies

- How you will evaluate the effectiveness of your awareness activities.

Determine your target audience

Target groups will include stakeholders (client groups, contractors, suppliers, consultants, community) who deal with the organisation and who are likely to have an impact on the organisation's operations. They also include those who may be affected or disadvantaged by fraud and corruption within the organisation because of their client relationship.

The outcomes of the risk identification and assessment process provide good starting points (see Chapter 2). They will give a picture of the potential risks as well as likely audience groups and their links with various activities or functions.

Once these risks and groups are defined, the delivery mechanisms and desired messages about the organisation's stance on fraud and corruption should be matched with the audience. In many cases there will be overlaps, and practical resource considerations will always govern the scope of these activities. The important thing to remember is to always communicate with the audience at the grassroots level and in a way that it most readily understands and accepts.

Refine your key messages

Fraud and corruption control awareness should be built around a variety of messages, presented in ways that ensure freshness and consistency.

The messages should stand alone as well as being embedded in all organisation communications and interactions with the external community.

Some of the basic functions of these messages should be:

- setting boundaries and expectations that fraud, corruption and any other forms of dishonest, unethical or criminal behaviour will not be tolerated
- promotion of positive values and the benefits of ethical business practices
- showing that the organisation is committed to best practice and honest and equitable services
- outlining steps the organisation has taken to prevent and detect fraud and corruption, regardless of where the threats may arise
- demonstrating the organisation's resolve to take forthright and impartial action against any party that breaches acceptable best practice in their dealings with the organisation
- outlining the opportunities for reporting unacceptable practices.

Communication methods

The communication strategies should be tailored according to the organisation's specific risks, its stakeholders and the target audience. The CCC website gives examples of promotional and training materials and links to other useful sites. The CCC also provides expert advisory services on policy, communication and change management through its experienced prevention officers.

Some communication options to consider include:

- making codes of conduct easily available for the public
- promoting ethical practices and values statements, such as making them prominent on website home pages

- incorporating suitable messages in external presentations, such as leadership and service group speeches, in the organisation's promotional materials and in annual reports
- sponsoring appropriate community activities that promote good governance
- incorporating ethical standards and requirements in job advertisements and procurement documentation clearly indicating expected organisation responses and procedures for clients (e.g. procedures for receiving cash payments, timelines for decisions and performance pledges)
- prompting clients to question any procedures until they are satisfied that there has been no inappropriate behaviour by the organisation or its officers
- including explanatory best-practice statements in documentation to contractors and suppliers
- incorporating recoupment (sometimes called "claw back" provisions) and other ethical practice provisions in contracts
- providing responsive advisory and client relation services including a public complaints hotline
- providing fraud prevention stories in client communications and for the media
- incorporating suitable fraud and corruption control materials on the organisation's website
- taking suitable action when encountering wrongdoing, and being honest and transparent in acknowledging the issues and the corrective measures that are being taken.

It is important to remember that communication is an ongoing and two-way process. The organisation and its employees constantly interact with stakeholders and send messages in subtle ways that influence attitudes and beliefs. The process never stops because it is continually being improved. However, from a practical viewpoint, communication programs normally consist of specific activities or discrete projects or events.

Messages are reinforced by repetition. Their frequency and method of delivery will depend on:

- the type of communication
- the relevance of the message to the person receiving it
- the financial or other impact of the desired behaviour change.

The key to having the receiver retain messages is to send them in a variety of creative and cost-efficient ways, while maintaining a consistent philosophical approach.

Some common dangers in developing awareness

Pitfalls to avoid include:

- defining the communication and awareness process too narrowly
- not thinking strategically in defining the messages, targets and delivery mechanisms
- treating awareness and communication as an afterthought or optional add-on
- not committing sufficient resources to the task
- using communications inappropriately.

Providing clear guidelines to external service providers

Consider the following measures to ensure that external service providers meet expected standards of accountability:

- develop appropriate contractual conditions and access provisions to ensure that performance, accounting and security requirements are met
- provide the organisation's fraud control policy to external service providers

- establish monitoring and reporting arrangements, providing a flow of information between the parties, so that organisations are well placed to assess their performance under contractual arrangements.

Regardless of how effective the external awareness program may be, its impact will be diminished if the organisation or its employees behave unethically, or if the community thinks that the organisation does not deal with corruption properly.

Conversely, when stakeholders have first-hand experience and see direct evidence of ethical behaviour on the part of the organisation and its employees, the reputation of the organisation is enhanced. Good performance strengthens public confidence in the organisation, its employees and its activities.

The organisation's real behaviour, good or bad, and not the rhetoric of the communications program, will be the ultimate determinant of the organisation's reputation and ability to serve the public interest.

Monitoring the outcomes

External communication effectiveness can be monitored by asking for feedback from target groups. This should be designed to explore their understanding of the organisation's stance on fraud and corruption and what control and prevention measures exist.

Awareness is an exceptionally fluid concept, and the communication plans or awareness-raising programs should be subject to regular review to ensure they retain their relevance. These reviews should seek input from all stakeholders to identify areas for improvement. These improvements may extend beyond the organisation's communication activities, and include better ways of recognising and addressing potential fraud and corruption issues as they arise.

Best-practice target

(1) The organisation should have an ongoing external awareness program that broadcasts to all its stakeholders its commitment to honest and ethical business practices and the measures it has adopted to prevent, detect and respond to both internal and external fraud and corruption.

(2) The program should target all stakeholder groups, including suppliers, clients and the general community.

(3) The messages conveyed by the program should make it clear that:
- the organisation is committed to best practice
- fraud and corruption are not acceptable to the community or the organisation
- wrongdoers will be subject to appropriate disciplinary action and prosecution.

(4) The content should include the enhancement of ethical practices generally, as well as focused communications to address the specific needs of client or industry groups, or particular organisational functions.

(5) The program should use a variety of delivery mechanisms, to ensure freshness of the underlying messages.

(6) The program should include mechanisms for dialogue with and feedback from its target audience.

(7) The program should be constantly monitored and regularly evaluated to ensure its continuing relevance and effectiveness.

Checklist: Client and community awareness program

The following questions are indicative only. Each organisation should develop its own checklist to reflect its specific needs and risk environment. The checklist should be re-examined and updated periodically, as part of the organisation's program of fraud and corruption control appraisal.

Legislative requirements

Has the organisation arranged for the general public to have easy access (RTI Act section 3) (for example, via the organisation's public website) to the following key documents:

- ☐ fraud and corruption control policy/plan?
- ☐ code of conduct?
- ☐ purchasing policies and procedures?
- ☐ gifts and benefits policy?
- ☐ register of all gifts or benefits with a retail value of more than $150 received or given by officers of any public service department or agency (PSC Directive No. 22/09)
- ☐ financial statements?
- ☐ annual reports?
- ☐ complaints policies?
- ☐ PID procedures? (PID Act section 28 (2))

Recommended Best Practice

- ☐ Has the organisation implemented an external awareness program covering the control and prevention of internal and externally initiated fraud and corruption?
- ☐ Does the program cater for all identified target groups?
- ☐ Is this awareness program comprehensive and pervasive?
- ☐ Does the organisation use a variety of appropriate presentation and delivery mechanisms for the program?

Has the organisation enhanced its public information and community relations role by publishing information about:

- ☐ actions taken in response to identified fraud and corruption situations?
- ☐ economies and/or improvements to performance or levels of service as a result of improved fraud and corruption control practices?
- ☐ Has the organisation enhanced its fraud and corruption management by engaging (either as an organisation or through the commitment of individuals) in more general public information activities and promotional ventures oriented towards minimising fraud and corruption risk?
- ☐ Does the annual report include a clear statement of the organisation's stance on fraud and corruption as well as its fraud and corruption control program and any initiatives taken during the year in question?
- ☐ Do appropriate public spaces of the organisation, including websites, carry notices about organisational values, probity or performance pledges consistent with a transparent and accountable organisation?

- ☐ Does the organisation highlight ethical considerations in job advertisements, position statements and procurement documentation?
- ☐ Has the organisation developed a supplier and contractor document covering best practice in business dealings with the organisation?
- ☐ Is a copy of the organisation's code of conduct provided as part of tendering documentation?
- ☐ Does the organisation's tender and contract documentation carry appropriate warnings against fraud or corruption such as the suspension or recall of contracts for improper business practices?
- ☐ Does the organisation explicitly state in its communications that it welcomes complaints or constructive feedback?

Does the organisation monitor its awareness program through surveys and other means to determine whether awareness and attitude change activities have been effective in:

- ☐ enhancing the organisation's image generally, and with stakeholder groups in particular?
- ☐ enhancing the self-esteem and job satisfaction of employees?
- ☐ deterring and/or detecting externally initiated fraud and corrupt approaches from suppliers, contractors or other external groups?

References

Attorney-General's Department 2017, Commonwealth fraud control framework, Australian Government, Canberra <www.ag.gov.au/CrimeAndCorruption/FraudControl/Documents/CommonwealthFraudControlFramework2017.PDF>

Attorney-General's Department 2017, Resource Management Guide No. 201 Preventing, detecting and dealing with fraud, Australian Government, Canberra. <www.ag.gov.au/CrimeAndCorruption/FraudControl/Documents/FraudGuidance.pdf>

Brown, AJ, Mazurski, E and Olsen, J 2008, *The incidence and significance of whistleblowing in Whistleblowing in the Australian Public Sector*, ANU Press, Canberra. <http://epress.anu.edu.au?p=8901>

Campbell, Nancy, 1998, *Writing effective policies and procedures: a step-by-step resource for clear communication*, American Management Association, New York.

Code of Conduct for the Queensland Public Service.

CCC — see Crime and Corruption Commission.

Committee of Sponsoring Organizations for the Treadway Commission 2016, *Fraud Risk Management Guide,* American Institute of Certified Public Accountants, Jersey City.

COSO: See Committee of Sponsoring Organizations for the Treadway Commission.

Crime and Misconduct Commission 2004, *Profiling the Queensland public sector: risks and misconduct resistance strategies survey*, CMC, Brisbane.

Crime and Corruption Commission 2016, *Corruption in focus: a guide to dealing with corrupt conduct in the Queensland public sector*, CCC, Brisbane.

DPC — see Department of the Premier and Cabinet.

Department of the Premier and Cabinet, *Annual Report requirements for Queensland Government agencies*. <www.forgov.qld.gov.au/manage-government-performance>

—— 2009, *Integrity and Accountability in Queensland*. <http://pandora.nla.gov.au/pan/40556/20150112-0000/www.premiers.qld.gov.au/publications/categories/reviews/integrity-and-accountability-reform/assets/integrity-and-accountability-paper.pdf>

—— 2009, *Response to Integrity and Accountability in Queensland*. <https://cabinet.qld.gov.au/documents/2009/Nov/Integrity%20and%20Accountability%20Reforms/Attachments/response-to-integrity-accountability.pdf>

Department of Finance, Risk Resources. < www.finance.gov.au/comcover/policy/risk-resources.html>

Financial Accountability Handbook, Info Sheet 3.15.

G20 Anti-Corruption Action Plan Action Point 7: *Protection of Whistleblowers*, 2011. <www.oecd.org/g20/topics/anti-corruption/48972967.pdf>

ICAC — see Independent Commission Against Corruption.

KPMG 2011, *Australia and New Zealand Fraud and Misconduct Survey*, 2010.

Public Sector Commission 2013, *Guideline 01/13: Discipline.*

Queensland Audit Office 2012, *Auditor-General of Queensland Report 5: 2012 Results of Audits: Internal control systems*, QAO Brisbane. <www.parliament.qld.gov.au/Documents/TableOffice/TabledPapers/2012/5412T401.pdf>

Queensland Ombudsman
<www.ombudsman.qld.gov.au>

Queensland Treasury 2011, *A Guide to Risk Management*
<www.treasury.qld.gov.au/resource/guide-risk-management/>

Queensland Treasury 2012, *Audit Committee Guidelines – Improving Accountability and Performance*.
<www.treasury.qld.gov.au/resource/audit-committee-guidelines-improving-accountability-performance/>

Queensland Treasury Financial Accountability Handbook.
<www.treasury.qld.gov.au/office/knowledge/docs/financial-accountability-handbook/index.shtml>

Queensland Treasury, *Financial Management Tools*, October 2012.
<www.treasury.qld.gov.au/resource/financial-management-tools/>

Roberts et al. 2009, *Whistling while they work: towards best practice*. <www.griffith.edu.au>

Australian Standards

AS 8001:2008, Corporate Governance – Fraud and Corruption Control

AS/NZS ISO 31000:2009, Risk management – Principles and guidelines

ASA 240, Auditing Standard ASA 240 – The Auditor's Responsibilities Relating to Fraud in an Audit of a Financial Report

Legislation

Auditor-General Act 2009

City of Brisbane Act 2012

Crime and Corruption Act 2001

Criminal Code Act 1899

Financial Accountability Act 2009

Financial and Performance Management Standard 2009

Information Privacy Act 2009

Information Standard 18: Information security

Information Standard 31: Retention and disposal of public records

Information Standard 40: Recordkeeping

Integrity Act 2009

Local Government Regulation 2012

Police Service Administration Act 1990

Public Interest Disclosure Standard No. 1 – Queensland Ombudsman 2013

Public Interest Disclosures Act 2010

Public Sector Ethics Act 1994

Public Service Act 2008

Right to Information Act 2009

Websites

Committee of Sponsoring Organisations of the Treadway Commission (COSO) <www.coso.org>

Commonwealth Attorney-General's Department <www.ag.gov.au>

Corruption Prevention Network, Queensland (CPNQ) <www.cpnq.org>

Crime and Corruption Commission (CCC) <www.ccc.qld.gov.au>

Public Service Commission <www.psc.qld.gov.au>

Queensland Audit Office <www.qao.qld.gov.au>

Queensland Integrity Commissioner <www.integrity.qld.gov.au>

Queensland Ombudsman <www.ombudsman.qld.gov.au>

Queensland Police Service <www.police.qld.au>

Queensland State Archives <www.archives.qld.gov.au>

Queensland Treasury <www.treasury.qld.gov.au>

Standards Australia <www.standards.org.au>

Transparency International <www.transparency.org>

Other recommended references and reading

Crime and Misconduct Commission 2004, *Managing conflicts of interest in the public sector Toolkit*, CMC, Brisbane.

Crime and Misconduct Commission, Queensland Ombudsman and the Public Service Commission 2011, *Managing a Public Interest Disclosure Program*, CMC, QO, PSC Brisbane.

—— *Handling a Public Interest Disclosure*, 2011, CMC, QO, PSC Brisbane.

—— *Making a Public Interest Disclosure*, 2011, CMC, QO, PSC Brisbane.

Department of the Premier and Cabinet, 2009, *Response to Integrity and Accountability in Queensland*, Brisbane. <https://cabinet.qld.gov.au/documents/2009/Nov/Integrity%20and%20Accountability%20Reforms/Attachments/response-to-integrity-accountability.pdf>

New South Wales Auditor-General 2015, *Fraud Control Improvement Kit: Managing your Fraud Control Obligations*. <https://www.audit.nsw.gov.au/ArticleDocuments/197/D1506583%20%20FINAL%20Fraud_Control_Improvement_Kit_February_2015%20whole%20kit.pdf-updated%20August2015.pdf.aspx?Embed=Y>

Public Service Commission, *Directive No.02/17 Managing Employee Complaints.* <www.qld.gov.au/gov/system/files/documents/directive-02-17-managing-employee-complaints_3.pdf?v=1490336869>

—— *Directive No. 01/17 Discipline*. <www.qld.gov.au/gov/system/files/documents/2017-01-discipline-guidelines.pdf?v=1490761902>

Queensland Audit Office 2013, *Report 9: Fraud Risk Management,* March.

Queensland Audit Office 2018, *Report 6: Fraud risk management*, February

Queensland Treasury 2016, *Information for Statutory Bodies*.
<https://www.treasury.qld.gov.au/resource/information-statutory-bodies-overview-applicable-legislation-policies-guidance-documents/ >

—— 2011, *A Guide to Risk Management*.
<www.treasury.qld.gov.au/resource/guide-risk-management/ >

—— 2012, *Internal Controls training*.
<http://treasury.govnet.qld.gov.au/internal-controls>

Crime and Corruption Commission
QUEENSLAND

Crime and Corruption Commission
GPO Box 3123, Brisbane QLD 4001

Level 2, North Tower Green Square
515 St Pauls Terrace, Fortitude Valley QLD 4006

Phone: 07 3360 6060
(toll-free outside Brisbane: 1800 061 611)
Fax: 07 3360 6333
Email: mailbox@ccc.qld.gov.au

www.ccc.qld.gov.au

Stay up to date

Subscribe for news and announcements:
www.ccc.qld.gov.au/subscribe

Follow us on Twitter:
@CCC_QLD

Follow us on Facebook