NSW GOVERNMENT
Family &
Community Services
Ageing, Disability & Home Care

Disability Resource Hub Disclaimer

The material on the Disability Resource Hub is for reference only. No claim or representation is made or warranty given, express or implied, in relation to any of the material. You use the material entirely at your own risk.

The material is provided as point-in-time reference documents. FACS does not maintain the material and does not undertake to ensure that it is accurate, current, suitable or complete.

Where conditions and warranties implied by law cannot be excluded, FACS limits its liability where it is entitled to do so. Otherwise, FACS is not liable for any loss or damage (including consequential loss or damage) to any person, however caused (including for negligence), which may arise directly or indirectly from the material or the use of such material.

Contents

Glossary

Disclaimer: The Department of Family and Community Services (FACS) does not warrant that these definitions are legally correct. Directors should seek professional legal advice relevant to their issues.

board – the governing body of a non-government organisation, made up of

Note: some organisations refer to the board as a management committee and to the directors as management committee members. The term 'board' is used in this manual to include management committee.

corruption – dishonest activity in which a person acts contrary to the interests of the organisation and abuses his/her position in order to achieve personal gain for themselves or for another party.

fraud – dishonestly obtaining a benefit by deception or other means.

fraud and corruption control plan – a document summarising an organisation's anti-fraud and anti-corruption strategies.

fraud and corruption risk assessment – identifying, understanding and documenting any potential risk of fraud and corruption within an organisation.

organisation – a company, firm, enterprise or association, or other legal organisation, whether incorporated or not, public or private, that has its own function(s) and administration.

policy – a general statement of a principle that guides decision making.

procedures – specific statements that detail what steps or actions are to be taken in a particular situation.

risk – the chance of something happening that will have an impact on the organisation's objectives. Risk is measured in terms of likelihood and consequences.

risk management – the process of identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them and monitoring and reviewing progress.

About this chapter

As a director, it is important to understand the fraud and corruption risks that your organisation could face. Fraud and corruption can undermine the viability of non-government organisations, compromise the delivery of services and breach the trust of stakeholders.

This chapter explores what fraud and corruption control is and how your organisation can take steps to prevent, detect and respond effectively to incidents of fraud and corruption.

The approach adopted in this chapter is based on the Australian Standard on Fraud and Corruption Control AS 8001:2008 *https://www.saiglobal.com/PDFTemp/Previews/OSH/AS/AS8000/8000/8001-2008.pdf*.

Policy checklists and other resources are included at the end of the chapter. These tools can be used by your board to develop your fraud and corruption control framework, and on an ongoing basis as required.

7.1 About fraud and corruption prevention and control

As a director of a non-government organisation, it is important to cultivate a governance culture and practice of risk management. We all like to think that fraud and corruption will not happen in our organisation. Unfortunately, the reality is that while most employees, volunteers and directors do the right thing, fraud and corruption does occur, and often at a time least expected. The operational, financial, social and reputational impact on your organisation, its purpose and the people it supports, can be significant.

Fraud and corruption:

- undermine the viability of non-government organisations
- compromise the delivery of essential services for some of society's most marginalised and vulnerable citizens; and
- breach the trust of stakeholders, sometimes irreparably.

Directors should take a zero tolerance approach to fraud and corruption and take steps to prevent them/either from happening.

Prompt detection and follow-through is essential.

If an organisation that is in receipt of government funding experiences fraud or corruption, in the spirit of fostering collaborative working relationships, it is advised to notify their funding agency to ensure that there is no impact on the conditions of funding. Disclosure allows the funding agencies to work with organisations to monitor and prevent the risk of these occurrences in the future.

	Importance	Yes	No	Comments/Actions
Employee awareness • Our directors, staff and volunteers are made aware of fraud and corruption. • Staff are provided with fraud awareness training during induction and regularly at appropriate intervals throughout employment with attendance monitored.	By providing employees with an awareness of fraud, they are in a better position to take the most appropriate action in those circumstances.			
Pre-employment screening • We have established a pre-employment screening policy, incorporating employment, qualifications, National Criminal History Records Checks (NCHRC) and reference checks for staff and volunteers that reflect mandatory requirements where needed. • The screening process covers senior management and employees (as well as volunteers where appropriate).	• Screening identifies potential issues and factors that may be indicative of fraud risk such as prior criminal convictions.			
Service user and community awareness • We have raised customer and community awareness of our organisation's efforts regarding fraud prevention and control.	• The community is aware that your organisation will not tolerate fraudulent or corrupt behaviour and has a channel for reporting any concerns.			
Disciplinary action • We have established a formal disciplinary action policy should there be a breach of the fraud control policy or a deviation from the fraud strategy.	• This creates a deterrent effect to employees by illustrating that all cases will be investigated and disciplinary action taken and aims to decrease the incidence of fraud.			

Corruption

Corruption is *"an act that includes:*

- any dishonest or improper use of position or resources, including the misuse of information or material acquired in the course of official duties – even where this misuse occurs when the person no longer undertakes those duties
- conduct by a person which might lead directly or indirectly to the dishonest or improper use of position by a person undertaking official duties
- conduct which might directly or indirectly interfere with the carrying out of responsibilities by a public official, including bribery or violence."

Commonwealth Fraud Control Guidelines
https://www.ag.gov.au/Publications/Documents/CommonwealthFraudControlGuidelinesMay2002/Commonwealth%20Fraud%20Control%20Guidelines%20March%202011.pdf

Corruption may involve fraud, blackmail, theft, embezzlement, tax evasion, illegal acts, forgery or obtaining financial benefit by vice.

7.1.3 The Australian Standard AS 8001:2008

The Australian Standard AS 8001:2008 Fraud and Corruption Control is a better-practice standard that many organisations adopt voluntarily to develop a robust approach to fraud and corruption control.

The implementation of fraud and corruption controls will differ among organisations, depending on their size, structure and the nature of their activities.

7.1.4 What is fraud and corruption risk management?

Fraud and corruption risk management is a proactive approach to mitigating the risks posed by fraud and corruption before they occur. Strategies and actions to successfully manage fraud and corruption include:

a) prevention – proactive measures designed to help reduce the risk of fraud and corruption occurring in the first place

b) detection – measures designed to uncover incidents of fraud and corruption when they occur

c) response – measures designed to take corrective action and remedy the harm caused by fraud or corruption.

7.1.5 Who is responsible for fraud and corruption risk management?

Board/audit committee oversight

The board has a responsibility to ensure that there are programs and controls in place to address risk, including fraud and corruption risk, as well as ensuring that these controls are effective.

The board provides leadership in creating a culture of risk awareness and management and ensures that controls to mitigate the risk of fraud and misconduct are in place. The board, together with management, has overall responsibility for setting ethical and responsible business practices. Both board and staff should agree on a code of conduct as a condition of their work with the organisation. The code of conduct defines expected behaviours. According to company and association law, directors are legally required to act in the best interests of the organisation, honestly and in good faith and with due diligence. Sound fraud and corruption practice assists directors meet these responsibilities.

It is good practice for a board to:

- conduct an annual fraud and misconduct risk assessment
- review and discuss issues raised during the organisation's annual fraud and misconduct risk assessment
- review and discuss the quality of the organisation's anti-fraud programs and controls
- establish procedures for the reporting and treatment of concerns regarding questionable accounting or auditing matters.

Senior management oversight

Responsibility for the implementation of the organisation's fraud and corruption risk management approach should be shared at senior levels. The chief executive officer, general manager or coordinator should be held responsible for modelling ethical behaviour and a culture that helps to prevent fraud and corruption. Perpetrators of fraud may justify their actions if they believe they are overworked or have a right to a higher wage. Senior leadership can play a crucial role in shaping the working environment and how employees experience the workplace.

People who oversee daily operations with a high likelihood of risk such as service managers and people performing internal audit functions also have anti-fraud and anti -corruption responsibilities. The internal audit manager, or the person performing this function, should be actively involved in planning activities to prevent, detect and respond to actual and suspected fraud and corruption.

7.1.6 How to approach fraud and corruption risk management

Effective fraud risk management provides an organisation with tools to manage risk consistent with regulatory requirements, the organisation's business needs and compliance expectations.

The prevention, detection and response fraud management framework is provided in the table below.

<table>
<tr><th colspan="3">Audit committee oversight
Executive and line management functions
Internal audit, compliance, and monitoring functions</th></tr>
<tr><th colspan="3">Assessment > Design > Implementation > Evaluation</th></tr>
<tr><th>Prevention</th><th>Detection</th><th>Response</th></tr>
<tr><td>• Fraud risk assessment
• Code of conduct and related fraud policies and standards
• Employee and third party due diligence
• Communication and training
• Process-specific fraud risk controls</td><td>• Hotlines and whistle-blower mechanism
• Auditing and monitoring
• Proactive forensic data analysis</td><td>• Internal investigation protocols
• Enforcement and accountability protocols
• Disclosure protocols
• Remedial action protocols</td></tr>
</table>

Source: KPMG LLP (US), 2006

The framework identifies four phases to fraud risk management:

- **Assessment** – identify the current state of fraud risk management, set targets for improvement and define steps necessary to close the 'gap'.
- **Design** – develop a program that encompasses controls to prevent, detect and respond to incidents of fraud and misconduct.
- **Implementation** – implement the new controls throughout the organisation and assign responsibility.
- **Evaluation** – assess the performance of the fraud and corruption risk management controls.

The fraud prevention control checklist (Resource 1) at the end of this chapter, can be used to identify control measures to help your organisation manage the risk of fraud.

7.2 The fraud and corruption control framework: prevention, detection, response

Prevention strategies

7.2.1 Code of conduct and related fraud policies and standards

Code of conduct

Organisations should have a code of conduct which clearly articulates the ethical standards that management and employees are required to follow. The code of conduct should be communicated across the organisation as well as to key stakeholders.

Developing and implementing a fraud and corruption control policy and plan

Organisations should develop and implement a fraud and corruption control policy and plan. A fraud and corruption control policy clearly articulates the organisation's stance on fraud and corruption.

A fraud and corruption control plan documents the organisation's approach to controlling fraud and corruption risk. It should detail the organisation's action plan to implement and monitor the organisation's fraud and corruption prevention, detection and response programme.

The fraud and corruption control plan should be part of an organisation's overall risk management plan (refer to Chapter 6 for risk management principles).

The board is responsible for the ongoing monitoring of the plan, the CEO is accountable for the implementation which can be delegated to a person with appropriate seniority, skills and experience and sufficient time.

A sample policy and plan template is provided at the end of this chapter (Resource 2).

7.2.2 Communication and training

An organisation should raise the awareness of directors, staff and volunteers of fraud and corruption risks including early warning signs and how to respond if fraud or corruption is suspected.

A significant proportion of fraud and corruption is not identified early because staff do not recognise the warning signs or are unsure how to report their suspicions.

Annual training sessions help raise awareness and also demonstrate the board and senior management's commitment to fraud and corruption prevention.

Fraud and corruption awareness can also be promoted through regular meetings, staff newsletters or other internal publications.

The following resources are provided at the end of this chapter to assist you with raising fraud and corruption awareness in your organisation:

- approaches for raising awareness (Resource 3)
- industry case study tool (Resource 4)

Some of the suggestions in (Resource 3) can also be used to raise fraud and corruption awareness amongst service users and the broader community.

7.2.3 Fraud and corruption risk assessment

Boards should engage with fraud and corruption risk assessment as a key prevention strategy.

A fraud and corruption risk assessment involves identifying key areas of exposure within your organisation and rating the likelihood and consequence of each risk. Once risks are identified and prioritised, the critical work involves identifying mitigating strategies as key control mechanisms to manage and monitor the risks.

Australian Standard AS/NZS ISO 31000:2009 identifies the seven stages of risk management:

a) communicate and consult

b) establish the context

c) identify risks

d) analyse risks

e) evaluate risks

f) treat risks; and

g) monitor and review.

(Refer to Chapter 6: Risk Management for further information)

A fraud risk self-assessment tool is provided at the end of this chapter to assist with your fraud and corruption risk assessment (Resource 5).

7.2.4 Employee and third party due diligence

Employee and third party due diligence is considered to be an effective way of reducing an organisation's potential exposure to internally based fraud and corruption. It is a condition of the provision of financial assistance under the Act that the requirements s32 relating to its relevant workers and relevant board members must be complied with.

> **TIP:** Under the *Disability Inclusion Act 2014* (NSW) (DIA) it is a requirement for disability service providers to screen potential staff to determine their suitability to provide home services to people with disability. Additionally, all people working in positions or preferred applicants for positions that involve child related work must have a Working with Children Check (WWCC) clearance from the Office of Children's Guardian.

Disability service providers are required to have a policy regarding the screening of staff. The policy must stipulate that all relevant workers and board members working directly with "the targeted group" (language used by legislation) in a way that involves face-to-face or physical contact, must undergo a National Criminal History Records Check (NCHRC) prior to commencing work. Those convicted of certain prohibited offences or who refuse to undertake a criminal record check must not be employed to work directly with targeted group. They are also required to get a reference, s32(3)(b) DIA. This check referee check must be completed every four years.

The objective of the screening process is to reduce the risk of potential security breach and to obtain assurance as to the integrity, identity and credentials of personnel and third parties dealt with by the organisation.

Employment screening should be considered for all new employees joining the organisation (including contractors) and all personnel being transferred to a senior executive position or to a position considered by the organisation to be 'high-risk' in terms of the potential exposure to fraud or corruption (for example, cash handling or procurement).

A typical employment screening process may include:

- verification of personal identity (using at least two forms of identity document such as a passport, birth certificate, drivers license)
- police criminal history search
- bankruptcy checks
- reference checks with the two most recent employers.

It is also important to consider any gaps in the employment history of a potential candidate and the reasons for these gaps.

Under the DIA the definition of relevant workers and board members, includes employees, volunteers, subcontractors, students (other than school students on work experience), and board or management committee members. A detailed definition can be found in Chapter 5, section 4.1 or s 32 of the DIA.

Aged care services receiving funding from the Commonwealth Government are required to comply with the *Aged Care Act 1997* (Cth). Under the Act, approved providers must ensure that all new staff, volunteers and key personnel (this includes directors and board members) have a current (within three years) National Criminal History Record Check.

7.2.5 Process-specific fraud risk controls

Internal controls play an important role in preventing and detecting fraud and corruption. Some recommended internal controls for common processes, such as purchasing, are set out in Resource 5.

Detection strategies

7.2.6 Hotline and whistle-blower mechanisms

Your fraud and corruption control framework should include internal and external reporting mechanisms for staff and volunteers to report suspected fraud or corruption.

Internal reporting mechanisms include reporting through line management or directly to a nominated individual who has responsibility for fraud and corruption control. An alternative is an external anonymous reporting hotline, to remove the barrier of non-reporting for fear of reprisal.

Australian Standard AS 8004:2003 Whistle-blower Protection Program for Entities recommends the implementation of a whistle-blower protection policy that encourages staff to report suspected fraud and corruption and provide protection for whistle-blowers. This policy should extend beyond staff and volunteers to suppliers, contractors and service users. The policy needs to be well communicated and understood and embedded into organisation culture and practice.

Organisations should consider providing external parties with an avenue to report suspected fraud or corruption. This can be achieved, for example, by extending the staff and volunteer reporting hotline to external stakeholders.

7.2.7 Auditing and monitoring

Auditing and monitoring processes can be effective in detecting transactions that are out of the ordinary. Auditing and monitoring is undertaken by an employee who is independent of the employee initiating transactions. Larger organisations have internal audit functions which perform this role.

Software tools are available which quickly scan large quantities of information for anomalous transactions and suspicious trends. These types of processes can integrate with existing IT systems.

Implementation of a budget and other performance indicators provides a guideline against which to measure financial performance and make a high-level determination as to whether income and expenditure is in line with strategy and expectations. The board and management should see regular financial reports against budget.

7.2.8 Proactive forensic data analysis

An organisation's information systems are an important source of information on fraudulent and, to a lesser extent, corrupt conduct. Software can identify suspect anomalous transactions for further investigation. Transaction analysis can also be undertaken using data analytics or manual review.

Response strategies

7.2.9 Advising funding agencies

Organisations who receive some of their revenue from government funding and experience fraud or corruption, should, in the spirit of fostering collaborative working relationships, notify their funding agency. This is to ensure that there is no impact on the conditions of funding and common approaches are identified to reduce risk.

Disclosure allows funding agencies to work with organisations to monitor and prevent the risk of future occurrences.

7.2.10 Internal investigation protocols

An investigation into actual or suspected fraud and corruption should be conducted by appropriately skilled, experienced and independent personnel. Organisations can choose to use external specialists if they do not have appropriately skilled staff who are independent from the area of fraud.

Investigations should be conducted according to the following principles:

a) natural justice and procedural fairness (see Chapter 2 – Legal Issues, page 19).

b) all parties should enter into confidentiality agreements in relation to the information coming into their possession during the course of the investigation.

c) any investigation resulting disciplinary proceedings should be conducted in an atmosphere of transparency, independence, fairness and objectivity at all times.

d) an investigation should comply with all relevant legislation.

e) adequate records to be kept of all investigations.

Any investigation should be subject to an appropriate level of supervision/ review by the board or a responsible committee with regard to the seriousness of the matter under investigation.

7.2.11 Enforcement, accountability and disclosure protocols

The investigator should submit a written report to the board detailing the circumstances and, where appropriate, recommending appropriate remedial or disciplinary action.

Once the board receives a report alleging fraud or corruption, they may decide to:

- deal with the matter as an allegation of misconduct using the organisation’s disciplinary process
- take remedial action immediately; or
- dismiss the allegation.

Organisations should have a policy on whether and how allegations of fraudulent and corrupt conduct should be reported to the police and other appropriate external parties such as a government body. The policy must comply with mandatory legal obligations which require certain matters to be reported to the police. Matters that must be reported include circumstances in which it appears there is evidence of fraud or corruption constituting a "serious indictable offence". *The Crimes Act (1900)* NSW states that a "serious indictable offence" is any offence that has a maximum penalty of five years imprisonment or more, for example theft, obtaining benefit by deception, embezzlement or misappropriation of money and bribery.

> **TIP:** For organisations providing disability services, the *Disability Inclusion Act* 2014 places a number of obligations on employers. Under the Reportable Incidents Scheme (governed by Part 3C of the Ombudsman Act 1974) with respect to reportable incidents service providers have 30 days to report any incidents to the New South Wales Ombudsman, from the time they became aware of the incident. If the incident involves a crime, it is important that the incident is also reported to the Police (refer to Chapter 2 – Legal Issues). Amongst the reportable incidents is deception and fraud related offences, abuse and neglect perpetrated by employees against persons with disability including children. A guide and forms to initiate this process are available at *http://www.ombo.nsw.gov.au/what-we-do/our-work/community-and-disability-services*.

Organisations should have a formal disciplinary action policy which can act as a deterrent to employees by stipulating that all cases will be investigated and disciplinary action will be taken against those staff that "do the wrong thing".

Where suspected or actual fraud or corruption exists, the organisation should undertake a formal process to form a view as to whether the matter is one that ought to be reported to the relevant law enforcement agency and the New South Wales Ombudsman for investigation and therefore, potentially, prosecution. The organisation's external reporting policy should be consistently applied so that there can be no suggestion of selective application.

A senior person within the organisation should maintain a record of all allegations of fraud and corruption and outcomes. (Refer to Resource 6 for a sample fraud incident register.)

7.2.12 Remedial action protocols

Recovery of proceeds of fraudulent conduct

Organisations should have a policy requiring that recovery action be undertaken where there is clear evidence of fraud or corruption and where the likely benefits of such recovery will exceed the funds and resources invested in the recovery action.

Organisations should consider taking out fidelity insurance to protect against funds misappropriated by staff and assist in the recovery of losses.

Media management

Organisations should have procedures to manage the media in the event of publication of fraud affecting the organisation. If the media are not handled appropriately, this can result in negative publicity and reputational damage to the organisation.

Internal control review

It is important to perform an internal control review in the area where the fraud occurred. This will help to ensure weaknesses and gaps in internal controls are addressed to prevent the fraud from reoccurring.

7.3 Conclusion

Effective fraud and corruption risk management is crucial to your organisation to enable you to deliver quality services to your service users and maintain the confidence of stakeholders. As a director, it is important to understand the fraud and corruption risks that your organisation could face and ensure that effective measures are in place to prevent, detect and respond to fraud and corruption.

References

Australian Standard AS 8001:2008 Fraud and Corruption Control Standards Australia
Phone: (02) 9237 6000
Email: *mail@standards.org.au*
Website: *www.standards.org.au*

Australian Standard AS 8004:2003 Whistle-blower Protection Programs for Entities
Standards Australia
Phone: (02) 9237 6000
Email: *mail@standards.org.au*
Website: *www.standards.org.au*

KPMG Fraud Risk Management White Paper
Developing a Strategy for Prevention, Detection and Response
KPMG
10 Shelley Street, Sydney NSW 2000
Phone: (02) 9335 7000

Resources

Resource 1: Fraud prevention and control checklist

DIRECTOR'S NOTES

This checklist can be used by the board to identify the areas to be considered in developing an approach to preventing, detecting and responding to fraud. Tick 'Yes' or 'No' and utilise the actions column to take notes.

	Benefit	Yes	No	Comments/Actions
Prevention				
Fraud and corruption control policy and plan • We have established and implemented an overarching fraud and corruption control policy and plan.	• The fraud and corruption control policy communicates the organisation's commitment to fraud and corruption control. The fraud and corruption plan sets out management's approach to preventing, detecting and responding to fraud and corruption.			
Ethical framework • We have a code of conduct or code of ethics which supports a zero tolerance of fraud and is communicated to all directors, staff and volunteers.	• Establishing an ethical framework, sets the boundaries for which staff are to operate in.			
Assign responsibilities • We have assigned responsibility for fraud and corruption to senior management.	• If responsibilities are clearly established and assigned, this will assist accountability for fraud control.			

	Importance	Yes	No	Comments/Actions
Employee awareness • Our directors, staff and volunteers are made aware of fraud and corruption. • Staff are provided with fraud awareness training during induction and regularly at appropriate intervals throughout employment with attendance monitored.	By providing employees with an awareness of fraud, they are in a better position to take the most appropriate action in those circumstances.			
Pre-employment screening • We have established a pre-employment screening policy, incorporating employment, qualifications, National Criminal History Records Checks (NCHRC) and reference checks for staff and volunteers that reflect mandatory requirements where needed. • The screening process covers senior management and employees (as well as volunteers where appropriate).	• Screening identifies potential issues and factors that may be indicative of fraud risk such as prior criminal convictions.			
Service user and community awareness • We have raised customer and community awareness of our organisation's efforts regarding fraud prevention and control.	• The community is aware that your organisation will not tolerate fraudulent or corrupt behaviour and has a channel for reporting any concerns.			
Disciplinary action • We have established a formal disciplinary action policy should there be a breach of the fraud control policy or a deviation from the fraud strategy.	• This creates a deterrent effect to employees by illustrating that all cases will be investigated and disciplinary action taken and aims to decrease the incidence of fraud.			

	Benefit	Yes	No	Comments/Actions
Internal control framework • We have established an adequate internal control framework, with well documented policies and procedures that are well communicated to staff and volunteers to support the fraud and corruption control framework.	• A strong internal control framework will help to prevent and reduce the opportunities of fraudsters to commit fraud.			
Leadership Culture • We provide regular communication to staff and volunteers on matters such as responsibilities for fraud control, what constitutes fraudulent activity and fraud detection measures.	• The visibility of senior management's commitment to fraud and corruption control will ensure staff and volunteers have respect for adhering to fraud and corruption policies. It is important that senior management drives the ethical framework by leading by example.			
Fraud risk assessments • We conduct regular fraud risk assessments to identify specific areas of fraud risk and develop appropriate countermeasures and action plans to address these risks.	• Regular fraud risk assessments assist in identifying new and emerging risks so that the appropriate control mechanisms can be put in place to prevent the fraud and corruption.			

	Importance	Yes	No	Comments/Actions
Detection				
Communication • We communicate our fraud detection initiatives to our staff and volunteers.	• Communication of fraud detection initiatives can act as a deterrent to an employee or volunteer contemplating fraud.			
Policy • We have a policy to investigate all reports of fraud.	• This creates a deterrent effect for employees.			
Responsibilities • Our staff, volunteers and directors know what to do if they suspect fraud or corruption.	• Reporting avenues should be well known by all employees and reporting should be encouraged, to ensure that suspicions or incidences of fraud and/or corruption are reported to management in a timely manner.			
Reporting • We have implemented fraud reporting channels which provide employees with both internal and external reporting options that encourage and enable staff to report suspected and known fraud. We have considered the establishment of a whistle-blower hotline service to encourage anonymous reporting external to the organisation.	• In some instances, staff and volunteers may not feel comfortable reporting matters internally due to fear of reprisal. An anonymous external hotline allows the organisation to capture those reports that may not otherwise be received.			

	Importance	Yes	No	Comments/Actions
Third party reporting - My organisation encourages third parties to make reports (i.e. service users, suppliers, contractors, partners) by providing information about how to make such a report.	- Extending reporting avenues to third parties helps identify suspicions or incidences of fraud that may potentially be undetected by employees or volunteers.			

	Benefit	Yes	No	Comments/Actions
Disclosure protection • My organisation makes a clear commitment to supporting and protecting all employees and volunteers reporting suspected or actual incidences of fraud so far as is legally possible and encourages employees to make disclosures. This policy extends beyond employees and volunteers to suppliers, contractors or service users.	• This encourages the reporting of suspected or actual incidences of fraud so that appropriate action can be taken without fear of reprisal.			
Detection systems (if applicable) • We have considered the use of detection systems such as employing the use of computer systems to detect fraud (data mining and real time transaction monitoring).	• Detection systems help to detect incidences of fraud early so that action can be taken to reduce the severity of the fraud and help implement controls to prevent its reoccurrence.			
Reporting to the board • We have a policy for reporting to the board, funding agencies and any other relevant authority all instances of suspected fraud and corruption.	• The governing body is aware of any incidences of fraud so that necessary changes can be implemented to prevent its reoccurrence.			

	Benefit	Yes	No	Comments/Actions
Reviews conducted • Management accounting reports are reviewed for signs of fraud and unusual trends. Post transactional review is performed for unusual transactions.	• Regular review will help detect any fraudulent activity so any necessary action can be taken to prevent its reoccurrence and reduce the severity of the suspected fraudulent activity.			
Fraud register • We maintain a register of all fraud reported and action taken.	• This will help to keep track of an organisation's risk exposure and highlight areas where fraud has occurred so that appropriate action(s) can be taken in order to control these risks of fraud from occurring again.			

	Importance	Yes	No	Comments/Actions
Response				
Skilled investigators • All investigations are conducted by well-qualified persons and outsourced where those skills do not exist in-house.	• It is imperative that investigations are carried out methodically by experienced investigators to ensure that evidence is not compromised.			
Media procedures • We have procedures to manage the press/media/shareholders/other stakeholders in the event of publication of fraud affecting the organisation.	• If the media are not handled appropriately, this can result in reputational damage to the organisation.			
Internal control review • My organisation performs an internal control review in the area where the fraud occurred.	• This will help to ensure internal control weaknesses and gaps are addressed to prevent the fraud from reoccurring.			
Fidelity and crime insurance • My organisation has fidelity insurance to protect against funds misappropriated by senior management and employees (including volunteers) and crime insurance to protect against fraud by external parties.	• Fidelity insurance can assist in the recovery of funds misappropriated by staff, including losses incurred and legal/investigative costs.			

Resource 2: Example structures for a fraud and corruption control policy

Sample fraud and corruption control policy template

A fraud and corruption control policy sets out the organisation's position on managing the risks of fraud and corruption, including:

- stance on fraud and corruption
- senior management commitment
- expectations of employees and others to which the policy applies.

1. Policy statement

Provide a summary of the importance and benefit of a fraud and corruption policy to the organisation.

2. Purpose

This section provides the overall aim of this policy. For example:

"This policy aims to assist in the prevention, detection and response to fraud and corruption. The policy provides a clear and transparent statement of the organisation's commitment to protecting its service users, employees and standing within the community by effectively preventing, detecting and responding to fraud and corruption."

3. Key terms and definitions

Provide key terms and definitions used in this fraud and corruption policy.

4. Relationship with other organisational policies

List other organisational policies which should be read in conjunction with the fraud and corruption policy.

5. Applicability

Identify the scope of the policy –specify stakeholders that the fraud and corruption policy will apply to.

6. Our commitment

Define the organisation's commitment to minimising fraud and corruption. For example promoting a culture of:

- a 'zero tolerance' position in respect of fraud and corruption
- vigorously investigating all matters concerning suspected fraud and corruption
- seeking to recover losses sustained through acts of fraud or corruption through all available avenues.

7. Expectations and Culture

Detail the expected behaviours of all staff and stakeholders and define the values and culture the organisation aspires to maintain high standards of integrity, probity and accountability.

8. Roles and responsibilities

Include the responsibilities of fraud and corruption prevention in this section.

9. Policy administration

Include policy administration matters such as policy review date, policy owner and contact officers here.

Resource 3: Methods for raising fraud awareness among an organisation's personnel

DIRECTOR'S NOTES

This resource is intended to assist directors raise fraud and corruption awareness in their organisations. The checklist can be used by the board to identify effective ways to educate staff.

Why is raising awareness among staff and volunteers important?

The more that employees and volunteers are aware of, and take ownership of their obligations concerning fraud and corruption control, the greater the effectiveness of the organisation's fraud and corruption control plan. Ongoing communication, training and mechanisms for staff and volunteers will enable the practice of behaviours and attitudes that prevent risks.

Every staff member (management and non-management), including volunteers, should have a general awareness of fraud and corruption so as to enable them to recognise the 'red flags' of fraud and know how to escalate a potential issue.

Regularly communicate with staff and volunteers about:

- the types of behaviour that may constitute fraudulent or corrupt practice,
- the fraud detection measures that are in place and
- how fraudulent and corrupt practices within the organisation will not be tolerated.

The following table provides a range of communication strategies that can be used to raise awareness:

Method	Description	Currently in place	
		Yes/No	Supporting comments
Written anti-fraud and corruption policies/ code of conduct	We have a written anti-fraud and corruption policy and a code of conduct. We take steps to ensure that all staff and volunteers are aware of these documents		
Regular formal fraud awareness training	We provide our employees and volunteers with regular fraud awareness training appropriate to their level of responsibility, which includes the following as appropriate: • Face to face training, including interactive case studies, facilitates increased learning of core concepts and is generally supplemented by appropriate e-learning modules and assessments to ensure and test knowledge gained. Ethics and code of conduct/policies should also be tested on a regular basis. Training sessions should also be embedded in induction training.		
Intranet and internet communication	We publish our fraud control related policies, news, blogs, bulletins and other information regarding promoting fraud awareness on our intranet and on our web site.		

Method	Description	Currently in place	
		Yes/No	Supporting comments
Discussion groups and webinars	Our staff and volunteers attend discussion groups and/or webinars organised and run by a professional group leader. Employees and volunteers may be more receptive to discussion amongst their peers in small informal groups. It is important that the group leader is properly equipped to ensure the appropriate issues are discussed and that the correct advice and information is given to those attending.		
Instructional videos	We present our staff and volunteers with instructional videos and include case scenarios that can be used at training, presentations and seminars in order to provide an interactive and engaging learning environment for staff.		
Fraud awareness publications and posts	We run fraud awareness segments in our online internal publications. We bring fraud awareness to the attention of employees and volunteers through online newsletters, online links, blogs, best practice case studies and organisation statistics. Posters/print outs in the office can be used for anti-fraud messages		
Report investigations and disciplinary action against perpetrators	We report incidents of investigations and disciplinary action to our staff, ensuring we respect the rights of perpetrators, as a deterrent for employees and volunteers not to become involved in fraud.		
Annual report	We included a statement regarding our commitment to ethical practices and fraud and corruption prevention in our annual report. This raises awareness within the community that fraud and corruption will not be tolerated by the organisation.		

Resource 4: Industry case study exercises

Developed by KPMG (© 2010 KPMG)

Overview

A number of fraud and corruption scenarios, based on real life examples of fraud in the NGO sector, are provided in this resource. The thirteen case studies have been developed through consultation with a cross section of senior representatives from the NGO sector.

How to use these case studies

You may like to selectively use the case studies as an awareness raising resource :

- for discussion during team meetings; or
- as training exercises for staff to complete in small groups.

Trigger questions are provided with each case study as the basis for further group discussion.

Case study 1: Payroll

Who?	Payroll operations supervisor
What?	Stole over $900,000 47 unauthorised transactions
When?	Over a five year period
How?	Transferred money into their personal account Coded payments to redundancy and superannuation within the accounting system
Why?	Household renovations New car Gambling
What happened to the fraudster?	Two year jail sentence, criminal record None of the money recovered

Points to consider	
How could this have been prevented?	Segregation of duties between staff that have access to bank details, those that prepare bank transfers and those that authorise bank transfers Two authorisers required to make a bank transfer. Financial reports against budget are reviewed regularly and questioned. Extraordinary items such as redundancy must always be approved by senior management. Payroll reports should be reviewed and approved prior to processing to the bank by someone other than the payroll team.
How could this have been detected sooner?	Review of bank transfers by another individual. Review and pre-transfer approval of payroll reports.

Case study 2: Procurement

Who?	House coordinator for disability group home
What?	Stole over $2,000
When?	Over a two year period
How?	Amended purchase order for house furniture by changing delivery to personal home address Order processed through accounts, outside the line of segregation of duties Later it was discovered that the house coordinator had done that same thing in their previous job
Why?	Feeling undervalued “Getting back at the company”
What happened to the fraudster?	Employment terminated Fined and criminal record

Points to consider	
How could this have been prevented?	Pre-employment screening including reference checks and National Criminal History Record Check. For disability service providers this is mandated within Disability Inclusion Act (DIA). Ensure strict adherence to internal purchasing policy and delegations of authority.
How could this have been detected sooner?	Fraud awareness training for procurement staff so that colleagues are well equipped to see the “red flags” of potential fraudulent behaviour and report it

Cash study 3: Theft

Who?	Line manager
What?	Stole heaters valued at over $5,000
When?	Over a three month period
How?	Heaters stolen from store room and sold on eBay. The heaters were not registered on an asset register so the organisations were unable to easily track movements.
Why?	Greed
What happened to the fraudster?	Employment terminated Fined and criminal record

Points to consider	
How could this have been prevented?	Physical asset security such as locked storeroom of portable assets, with access on approval. Assign responsibility of high value assets to an individual.
How could this have been detected sooner?	Keep a register of where assets are located and perform regular stock counts to ensure all are accounted for on a regular basis.

Case study 4: Nepotism

Who?	HR manager
What?	Favouritism of relative in recruitment process
When?	2009
How?	HR manager hired a relative for a management role. The relative did not have appropriate skills or experience for the role.
Why?	A personal favour to the relative Relative was heavily in debt and needed a job
What happened to the fraudster?	HR manager cautioned Relative dismissed

Points to consider	
How could this have been prevented?	Ensure staff are aware of their responsibility to disclose potential conflicts of interest. Follow a proper merit recruitment process that involves more than one person in decision making. Consider involving an independent party in the recruitment process.
How could this have been detected sooner?	CV and background checks reviewed by more than one person

Case study 5: Management of client funds

Who?	Plan manager
What?	Stole approximately $10,000 of service user funds
When?	Over a four year period
How?	The Plan manager had full access to the personal bank accounts of the service user and withdrew service user funds from ATMs in small amounts over four years
Why?	Opportunity
Vulnerable service user who would not notice	HR manager cautioned Greed
What happened to the fraudster?	Employment terminated Prosecuted for stealing. Two year jail sentence given their position of trust Criminal record

Points to consider	
How could this have been prevented?	Provide regular fraud awareness training to staff and volunteers and reaffirm the organisation's ethics policy on a regular basis. Inform and educate service users and families about the organisation's commitment to fraud prevention and precautions aimed at preventing fraud. Additional internal controls around service user monies. A reporting procedure in place for service users and their families. Independent review of service user transactions.
How could this have been detected sooner?	Ensure and promote reporting process for service users and their families

Case study 6: Cheque payments

Who?	Line manager
What?	$15,000
When?	Over a two year period
How?	Line manager was making cheque payments to a "ghost supplier". The ghost company was linked to a bank account which the line manager controlled. Cheques required two signatories, however senior authoriser pre-signed cheques, allowing the line manager to create cheques for any value and payable to where he specified.
Why?	Opportunity Gambling problem
What happened to the fraudster?	Employment terminated Prosecuted for fraud and fined with a criminal record

Points to consider	
How could this have been prevented?	Cheques are only signed once completely filled in. Supporting invoices are sighted before payment is authorised. Ensure segregation of duties of those who prepare the cheque, process and authorise.
How could this have been detected sooner?	Regular review of cheque payments by independent staff member

Case study 7: Gift vouchers

Who?	Senior member of management
What?	Theft of gift vouchers worth $1,500
When?	Over a three year period
How?	Gift vouchers were allocated to senior management for rewarding exceptional performance from staff. One senior manager pocketed the vouchers for personal use while reporting back that the vouchers were given to employees. This occurred annually over three years.
Why?	Opportunity Greed
What happened to the fraudster?	Had to repay the $1,500 back to the organisation Employment terminated

Points to consider	
How could this have been prevented?	Tighter internal controls around use of gift vouchers e.g. register of allocations.
How could this have been detected sooner?	Use of an anonymous whistle-blower reporting hotline

Case study 8: Gifts and benefits

Who?	Purchasing manager
What?	$16,000
When?	Over a two year period
How?	Purchasing manager purchased cars for the company from a car dealer at inflated rates. Car dealership provided purchasing manager with kickbacks (holiday packages provided to his family each Christmas).
Why?	Opportunity Greed
What happened to the fraudster?	Employment terminated Matter reported to police and prosecuted for fraud Matter was investigated and the manager was fined and now has a criminal record

Points to consider	
How could this have been prevented?	Provide regular fraud awareness training and reaffirm the organisation's ethics policy on a regular basis. Segregation of duties. Procurement policy requiring multiple quotes when purchasing assets.
How could this have been detected sooner?	Annual review of market values by an independent party

Case study 9: IT procurement

Who?	IT manager
What?	Fraudulent purchase of IT stock worth $12,000
When?	Over a two year period
How?	IT manager purchased extra IT equipment through the company purchase process Sold the extra IT equipment on eBay for personal gain
Why?	Opportunity Greed
What happened to the fraudster?	Employment terminated Prosecuted for stealing/fraud Criminal record and fined

Points to consider	
How could this have been prevented?	Segregation of duties between those that order and those that receive the physical goods. Ensure strict adherence to internal purchasing policy and delegations of authority.
How could this have been detected sooner?	Regular analysis of IT expenditure may have detected upwards trend in spend or variance against budget

Case study 10: Payroll entitlements

Who?	Payroll manager
What?	$30,000 of staff superannuation monies misappropriated
When?	Over a two year period
How?	Payroll manager diverted staff superannuation entitlements to another account controlled by the payroll manager.
Why?	Opportunity – many employees do not regularly check their superannuation contributions or balance Greed
What happened to the fraudster?	Employment terminated Prosecuted for fraud Criminal record and a jail sentence of two years

Points to consider	
How could this have been prevented?	Segregation of duties
How could this have been detected sooner?	Review of audit logs on payroll transactions/data sheets Staff members encouraged to regularly review their payslips and superannuation contribution statements

Case study 11: Credit cards

Who?	CEO
What?	$28,000 of fraudulent credit card transactions
When?	Over a six year period
How?	Using the company credit card to purchase personal goods and services Lack of oversight – the company had an external book keeper who did not have direct reporting to the board
Why?	Opportunity Greed
What happened to the fraudster?	Employment terminated Prosecuted for fraud Large fine and criminal record

Points to consider	
How could this have been prevented?	Set limits on the credit cards to reduce exposure Fraud awareness training
How could this have been detected sooner?	Review of expenditure items such as items coded to cost centres and having the manager of that cost centre review the expenditure Anonymous whistle-blower reporting process

Case study 12: Fuel theft

Who?	Highly respected individual in the community who worked in business services
What?	$500 worth of fuel
When?	Over a two year period
How?	Stealing company diesel
Why?	Financial hardship due to gambling addiction
What happened to the fraudster?	Employment terminated

Points to consider	
How could this have been prevented?	Restrict access to the fuel tank Surveillance security in area holding high-value portable assets
How could this have been detected sooner?	Monitor fuel expenditure over time and identify unusual trends

Case study 13: Staff bonuses

Who?	Supervisor
What?	$7,000 worth of bonuses
When?	2009
How?	Bonus allocation system required supervisors to allocate bonuses to their team based on the performance of each staff member One supervisor made an arrangement with certain team members that he would allocate the highest discretionary bonus in return for a 50 percent split kickback
Why?	Greed Opportunity
What happened to the fraudster?	Supervisor and team members received disciplinary action Employment terminated

Points to consider	
How could this have been prevented?	Additional internal controls around the performance bonus system Fraud awareness training for staff
How could this have been detected sooner?	Review of the expected bonuses by an independent person outside that of the business unit Anonymous whistle-blower hotline process

Resource 5: Fraud and corruption risk assessment tool

How to use the fraud and corruption risk assessment tool

This assessment tool covers the fraud and corruption risks that can occur in a broad range of scenarios.

The assessment is a collection of:

(1) possible inherent fraud and corruption risks that might occur in a series of typical situations, and

(2) recommended control measures that could be used to address them.

The recommended control measures are a collection of good ideas that would apply to most situations most of the time. However, there is no “one size fits all” solution. Some recommended control measures may not suit your particular situation, especially small organisations.

- Focus on one fraud and corruption risk category at a time (one category per page e.g. Assets on page 47). Consider all inherent risks in the first column. Add any others you can think of.
- Consider each recommended control measure separately. Indicate in the third column “yes” or “no” as to whether or not that control is in place in your organisation.
- Indicate in the fourth column your risk assessment rating (Low, Moderate, High or Extreme).
- Add any other useful control measures that may occur to you that have not been included in this document, and apply the same rating process.
- Determine and document a strategy to address all recommended control measures that you rated as Moderate, High or Extreme.
- Through this assessment and prioritisation, you will get a sense of the vulnerability to fraud of your organisation as a whole.
- Most importantly, implement your strategies.

Risk assessment rating

Use the tables and scales below to assess the severity and the likelihood of each risk. Use the last table to combine the two and help you rate each risk as Low, Moderate, High or Extreme risk.

Likelihood	Descriptor	Description
1	Almost certain	Is expected to occur in most circumstances
2	Likely	Will probably occur in most circumstances
3	Possible	Might occur at some time
4	Unlikely	Could occur at some time
5	Rare	May occur in exceptional circumstances

Severity	Descriptor	Description
1	Intolerable	Ruinous impact on reputation, critical financial loss, permanent disruption to capability
2	Substantial	Major impact on reputation, major financial loss, ongoing disruption to capability
3	Moderate	Modest impact on reputation, high financial loss, some ongoing disruption to capability
4	Minor	Minor impact on reputation, medium financial loss, minor disruption to capability
5	Trivial	No impact on reputation, low financial loss, no disruption to capability

Risk Matrix		1 (intolerable)	2 (substantial)	3 (moderate)	4 (minor)	5 (trivial)
Likelihood	1 (almost certain)	EXTREME	EXTREME	EXTREME	HIGH	HIGH
	2 (likely)	EXTREME	EXTREME	HIGH	HIGH	MODERATE
	3 (moderate)	EXTREME	EXTREME	HIGH	MODERATE	LOW
	4 (unlikely)	EXTREME	HIGH	MODERATE	LOW	LOW
	5 (rare)	HIGH	HIGH	MODERATE	LOW	LOW

For example, see under Assets, on page 40, the second recommended control measure is ‘Maintenance of a portable equipment register to keep track of laptops etc’. Suppose you indicated “No” against “Control measure in place”. You would then consider how risky this situation is. If there are no laptops or any equipment of any significant value that staff take away from the office, you might rate the risk as Low. On the other hand, if there are, and equipment has gone missing in the past, you might rate it High.

Similarly, on another recommended control measure you may have indicated that the control measure is in place. But you still need to determine the level of risk. For example, let us consider the first recommended control measure for Assets ‘New equipment valued >$500 immediately given an asset number and placed in assets register etc’. Although an asset register exists, it may not have been updated for some time, so you might rate it Moderate.

Administration

Fraud and corruption risk category – Assets

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
• Theft of assets, particularly "attractive" or portable assets such as laptops or other computer equipment. • Unapproved removal or disposal of assets e.g. because of alleged damage. • Loss of control over assets by asset register not being maintained. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• New equipment valued >$500 immediately given an asset number/ placed in assets register. Assets tagged with the asset number.		
	• Maintenance of a portable equipment register to keep track of laptops, etc. that are used by individual staff on a temporary basis.		
	• Annual reconciliation of assets on hand (stocktake) to those in the assets register, performed by officer/s independent of receiving or recording function.		
	• Asset disposal to be approved by management, and details documented and retained.		
	• Adequate physical security of assets and premises.		
	• Adequate insurance coverage of assets and premises.		
	Alternative/additional control measures:		

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
• Unauthorised private use of motor vehicles. • Theft of vehicles from parking areas or while garaged at home. • Theft or exchange of accessories or tools. • Use of petrol card for private vehicle or unauthorised purchases. • Falsification of vehicle log. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• Policy to convey expectations to staff regarding careful and authorised use of the organisation's vehicles.		
	• Absences from workplace to be approved by supervisor.		
	• Regular reviews of vehicle log books.		
	• Regular reviews of purchases on petrol cards.		
	• Clearly understood approval mechanism for taking cars.		
	Alternative/additional control measures:		

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
• Theft or loss of physical resources such as paper, stationery, tools, etc. • Unauthorised use of taxi vouchers. • Inappropriate use of telephones (including mobile phones), photocopiers and portable and valuable items. • Fraudulent travel allowance claims. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• Organisation's code of conduct distributed to all staff.		
	• Internal policies made available to all staff.		
	• Monitoring of usage/expenditure rates on photocopying, taxis, mobile phones, etc.		
	• Retention of invoices for expenditure on above, and system to track expenditure and usage.		
	• All travel allowances are monitored for reasonableness, with any expenses supported with original receipts.		
	Alternative/additional control measures:		

Finance

Fraud and corruption risk category – Accounts payable

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
• False invoices accepted resulting in payment for goods not received. • Collusive practice between supplier and purchasing officer resulting in invoice price higher than approved on ordering. • System is manipulated resulting in EFT payments to non-existent supplier. • False staff travel claims submitted. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• Invoice prices are validated by supporting documentation such as requisitions and purchase orders.		
	• Where possible, segregation of duties between purchasing officer and officer authorising payment.		
	• All staff travel claims approved by the supervisor.		
	• Two signatures on cheques and signatures registered with the bank.		
	• Blank cheques are not signed.		
	• Payments made on the basis of original invoices, and documentation stamped “paid”.		
	• Accounts payable ledger reconciled monthly to the general ledger.		
	• Bank reconciliations performed monthly, and reviewed and signed off by someone independent of the preparer.		
	• Internet payment or funds transfer requires the authorisation of two designated individuals.		
	Alternative/additional control measures:		

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
• Revenue owing by service users for services provided may not be collected by the accounts receivable officer (particularly in regard to relatives or friends). • Revenue collected from service users for services provided may be misappropriated by collecting officer. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• Reconciliation of service users' fees receivable (based on clear records of services provided) to money actually received from service users, by a person independent of the collection process.		
	• Reconciliation of money received from service users to money actually banked, by a person independent of the banking process.		
	• Encourage regular electronic payments as an alternative to cash payments		
	Alternative/additional control measures:		

> **TIP:** Disability Service providers operating under the NDIS will be able to claim payments through the online NDIS Portal. This will eliminate the risk of payments not being received. However service providers will need to ensure systems are in place to connect to the portal and staff are trained to promptly claim payments. Data management and accuracy becomes an important aspect of the business model.

Finance

Fraud and corruption risk category – Petty cash and cash receipts

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
Use of petty cash for private purposes. • Submission of bogus petty cash claims. • Receipts not issued for money received. • Under-banking or failure to bank cash receipts. • Misappropriation of funds. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• Policy on what can be claimed through petty cash.		
	• Paying officer should stamp claims and receipts as “paid”.		
	• Claims not to be paid without authorisation.		
	• Petty cash claims should contain details of the item purchased and supported by a receipt.		
	• Adequate physical security over cash holdings e.g. access to locked box or safe and combination limited, safe locked, etc.		
	• Procedure in place to enable regular reconciliation between documentation, cash receipts and petty cash claims.		
	Alternative/additional control measures:		

Human resources management

Fraud and corruption risk category – Payroll

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
• Unauthorised appointments. • Unauthorised overtime worked. • Timesheets altered to increase hours, allowances, etc. • Payments above approved entitlements. • Overpayment of employees. • Fraudulent recording of attendance/time. • Leave taken exceeds entitlement. • Inappropriate rosters eg. favouritism, excessive staff. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• Limited access to payroll.		
	• Supervisors approve staff timesheets or attendance variation forms to payroll.		
	• Appropriate delegations and procedures for appointment of staff.		
	• Monthly management reports (signed off) showing changes to payroll including new hires, resignations, promotions and rates.		
	• Process in place to ensure data entry and data review done by different staff. This applies to both regular payroll and changes such as new employees pay rates, deductions, etc.		
	• Regular management reviews of rosters.		
	• Regular management reviews/reports of major cost fluctuations, e.g. overtime worked and annual leave accumulation > set levels.		
	• Payroll approved by management before processing to bank.		
	Alternative/additional control measures:		

Human resources management

Fraud and corruption risk category – Personnel

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
• Applications for employment using false personal details. • Collusion between staff to cover unauthorised absenteeism. • Stealing time e.g. conducting personal business during working hours. • Fraud committed through negligence as a result of manager/ supervisor not checking claims for payment. • Fraudulent worker's compensation claims. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• Policies for new staff, terminations and WH&S.		
	• Thorough reference checks carried out on new employees (at least 2)		
	• Copies of original documentation required to verify personal details including qualifications.		
	• Suspicion of fraudulent worker's compensation claims reported and investigated.		
	• All staff and volunteers undergo mandatory National Criminal History Record Check prior to employment and every four years, or as mandated by relevant legislation.		
	Alternative/additional control measures:		

Information technology

Fraud and corruption risk category – Information technology

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
• Intruders or unauthorised staff gaining computer access. • Exposure of confidential information. • Tampering with administrative/financial records. • Excessive internet browsing. • Illegal (pirate) software installed. • Loss of data following accident, resulting in people taking unfair advantage of situation (e.g. stealing assets not recorded, demanding inappropriate payments, etc). • Inappropriate internet funds transfer by unscrupulous employee. • Confidential internet banking details stolen and misused by outsiders. • Corruption of data by hackers. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• Computer users require unique passwords for access.		
	• No shared passwords.		
	• Passwords regularly reset.		
	• Restricted access to specific records e.g. payroll, general ledger.		
	• Physical security of computers at all times, particularly when office unattended.		
	• Computer users lock work stations when unattended for long periods e.g. lunchtime.		
	• Staff leaving the organisation have computer access deleted as soon as they have left.		
	• Rules conveyed around the use of the internet and regular checking of private internet usage, including reviews of monthly internet bills.		
	• Staff are not permitted to install illegal software (pirate) software.		
	• Restrict users' ability to install software.		
	• Regular backup and proper labelling and off-site storage of important systems and data.		
	• Suspicion of any email from someone unknown or untrustworthy – deletion without opening of any suspicious emails, particularly with attachments.		
	• Not opening, running, installing or using programs/files obtained from a person or organisation not known to be trustworthy.		

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
	• Scanning of new programs/ files for viruses before opening, running, installing or using them.		
	• Keeping computer up-to-date with anti-virus, firewall software and the latest patches.		
	• Installation of software that will filter spam email or use of an Internet Service Provider (ISP) that will filter spam prior to delivery at your inbox (spam filters are often included in anti-virus software).		
	For internet banking: • Restriction of internet banking access to a limited number of authorised individuals, whose passwords are confidential to them and changed periodically and deletion of access when those people leave the organisation.		
	• Requirement for internet funds transfer to have the approval of two designated individuals.		
	• Not providing personal details including customer ID or passwords in response to any email (a bank will never ask you for any private password and this important information should never be shared with anyone).		
	• Not clicking on a link or attachment in an email which purportedly sends you to a bank's website. Access your bank's internet banking logon page only by typing the address into your browser.		

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
	• Use of passwords or PINs (Personal Identification Numbers) that are easy to remember but hard to guess. They should not be relevant to your personal or work situation. Passwords with telephone numbers, postcode, your name or the name of a close relative or work colleague, and dates of birth are simple for criminals to trace. Creation of passwords with letters and numbers that cannot be easily attributable to you or your organisation.		
	• Memorisation of your password or PIN and not writing it down or storing it on your computer, including in any system or on the programmable function keys. (You are responsible for keeping this information confidential, even from relatives and friends).		
	• Changing passwords regularly and not using the same password for other services.		
	• Confirming that your data is encrypted between your computer and the bank by looking for the key or padlock symbol on the browser window.		
	• Always logging out from internet banking when you finish all of your banking.		
	• Closing your internet browser after logging out at the end of each internet banking session.		

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
	• Being aware of any windows that 'pop up' during an internet banking session and being very suspicious if it directs you to another website which then requests your customer identification or password.		
	• Avoiding using shared computers at public places, such as internet cafes, to conduct your Internet banking.		
	• Looking after your account details if you save or print them after electronically accessing them from the bank's system. Keeping this information in a safe and secure place or destroying it once you have finished with it.		
	• Always checking your statements for any transactions that look suspicious. (If you see any transactions that you did not undertake, immediately report this to your bank).		
	• Being aware of scam emails that purport to be from a bank or another legitimate business, asking for confidential information or payments.		
	Alternative/additional control measures:		

Procurement

Fraud and corruption risk category – Inventory (stores)

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
• Theft of goods/ equipment. • Goods taken for personal use. • Unauthorised disposal of goods. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• Adequate physical security maintained for stationery, equipment and assets.		
	• Regular reviews of the reasonableness of asset and stationery requisitions.		
	• Regular stocktakes with results documented and reported to line management.		
	• Persons independent of the stores to be involved in stocktakes where possible.		
	• Line management approval required for disposal.		
	Alternative/additional control measures:		

Procurement

Fraud and corruption risk category – Purchasing

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
• Staff with a personal/ pecuniary interest in purchase or contract. • Collusive practices between supplier and purchasing officer. • Purchase of goods for private use. • Officers with delegation for requisition/purchase orders also signing for goods delivery. • Orders fraudulently changed. • Kickbacks or spotting fees paid to staff for preferential selection. • Purchasing through the internet via a fake website, resulting in theft and misuse of your credit card details. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• Personal and/or pecuniary interests are declared and registered including any interest in any firm with which your organisation conducts business.		
	• Procurement policy in place which includes requirement to obtain quotes from multiple suppliers and an independent approval process for selection of suppliers for purchases over an agreed amount.		
	• Limited access to purchase requests and orders and (where IT systems exist) to input screens for purchase requests or orders.		
	When purchasing online:		
	• Dealing only with approved, trusted suppliers that are verifiable and have secure e-commerce sites		
	• Not sending your credit card details via insecure means such as email that is not encrypted.		
	Alternative/additional control measures:		

Other

Fraud and corruption risk category – Service user operations

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)
• Inappropriate secondary employment: e.g. staff provide additional services to service user in return for cash. • Staff member accepts personal gift or benefit from service user without declaring (includes bequests). • Theft of service user monies (e.g. cash or EFT). • Staff member fraudulently uses service user funds for an alternative purpose. • Staff member uses their personal store loyalty card to collect frequent flyer points for service user transactions. • Staff member seeks a gift or benefit from a service user. Additional inherent risks: • Additional risk 1 • Additional risk 2 • Etc.	• Secondary employment policy		
	• Gifts and benefits policy		
	• Gifts and benefits register		
	• Service user funds policy		
	• Service user awareness mechanisms		
	• Management oversight of service user funds process		
	• Segregation of duties among staff dealing with service user funds		
	Alternative/additional control measures:		

Other

Fraud and corruption risk category – Other

[You should use this section to set out other fraud and corruption risk areas that your organisation may be exposed to.]

Inherent risks – what could go wrong	Recommended control measures	Control measure in place (yes/no)	Risk rating (High/ Medium/ Low)

Overall fraud and corruption risk assessment rating

Fraud and corruption risk category	(1) No. of control measures rated in each category	(2) Transfer from each fraud risk category
Administration		
Assets		
Motor vehicles		
General resources		
Finance		
Accounts payable		
Accounts receivable (service users' fees) Petty cash and cash receipts		
Human resource management		
Payroll		
Personnel		
Information technology		
Procurement Inventory (stores) Purchasing		
Other		
Service user operations		
Other		
Total		
	Overall fraud and corruption risk exposure Divide total of (2) by total of (1)	

Fraud and corruption risk action plan

[This template is provided to assist your organisation in planning to better manage fraud and corruption risks. Initially, you should focus on those risks with the highest ratings.]

	Risk	Proposed action	Responsibility	Due date
	Detail the relevant risk here. (e.g. staff member seeks a gift or benefit from a service user)	*Identify an action that your organisation could use to better manage this risk (e.g. implement a gifts and benefits policy and communicate the policy to all staff at the next team meeting)*	*Allocate a responsible person*	*Determine a due date*
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

Resource 6: Fraud register template

DIRECTOR'S NOTES

The purpose of this register is to record all reported allegations and/or identified instances of fraud and the response/actions taken by your organisation. It is a sample fraud incident register which you may find useful in deciding what style of register works best for your organisation. This register complements other documentation to record the details of each allegation of fraud.

Date of notification or identification of matter	Nature and key details of the matter	Estimated or actual value	Detection method	Response/ investigation strategy	Delegated officer	Escalation	Investigation outcome/ response

Explanatory notes

Nature and key details of the matter: Include details of what happened, how it occurred and who was directly involved in the alleged incident (if known).

Estimated or actual value: Identify both financial and other potential impacts, for example, reputation risk.

Detection method: Include details of the specific internal control, individual or process (or combination thereof) responsible fo identification of the alleged incident.

Response/investigation strategy: Include details of the proposed investigative response (for example, internal or external investigation and escalation approach) and other actions taken to ensure that the alleged fraud or similar fraud will not reoccur.

Delegated officer: Identify the officer responsible for the response/ investigation strategy.

Escalation: Identify the key parties who may need to be informed (if any) including management, Audit Committee, ICAC, insurer, law enforcement, etc.

Investigation outcome/response: Identify the final outcome and document proposed response, for example, disciplinary action, control enhancement, awareness raising