ORGANISATION Fraud Control Plan

DOCUMENT HISTORY, APPROVAL and REVIEW DETAILS

Date	Version	Author	Owner	Approved by	Reason for update

Dated approved		**Review frequency**		**Next Review Due:**	

Contents

1 EXECUTIVE SUMMARY

1.1 Introduction

The Fraud Control Plan (FCP) serves several purposes, all of which come under the umbrella of assisting (ORGANISATION) in preventing, detecting and deterring the risk of fraud. This plan has been developed with reference to *Australian Standards 8001 – 2008: Fraud and Corruption Control*.

In line with this guidance the plan has been structured in the following strategies:

a) preventing;
b) detecting;
c) investigating; and
d) recording and reporting.

The objective of the Fraud Control Plan is to minimise the potential for instances of fraud on (insert name of ORGANISATION) involving employees, contractors or people outside of the organisation. The Fraud Control Plan also articulate ORGANISATION's approach to controlling the risk of fraud through:

- thorough and regular assessment of the risk of fraud;
- developing and implementing processes and systems to effectively prevent, detect and investigate fraud;
- applying appropriate criminal, civil, administrative or disciplinary action to remedy the harm from fraud and deter future fraud;
- recovering proceeds of fraudulent activity; and
- providing fraud awareness training for all staff.

1.2 Definition of Fraud

ORGANISATION has adopted the definition of fraud provided by *Australian Standards 8001 – 2008: Fraud and Corruption Control*:

> *"Dishonest activity causing actual or potential financial losses to any person or entity, including theft of monies or other property by employees or persons external to the entity, where deception is used at that time, immediately before or immediately following the activity. This also includes deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit. "*

1.3 Statement of attitude towards fraud

ORGANISATION, regards and treats fraud seriously. All personnel, comprising staff and contractors, are responsible for ensuring strong, robust and effective fraud control. XXXX is committed to protecting its money and property from any attempt, either by members of the public, contractors, sub-contractors, agents, recipients, intermediaries or its own staff, to gain by deceit, financially or through other benefits.

In this regard, ORGANISATION:

- requires that any case of suspected or detected fraud must be reported immediately;
- commits to investigating suspected or detected fraud and taking appropriate action;
- adopts a risk management approach to the prevention, detection and investigation of suspected fraudulent activity that is incorporated into its business processes, management practices, internal controls and related activities;
- commits to training staff in fraud awareness annually; and
- undertakes appropriate action against those who have committed fraud.

1.4 Code of Conduct

ORGANISATION's Employee Code of Conduct expects all employees to follow and demonstrate professional and ethical work practices, including:

- always acting with honesty, courtesy and integrity;
- consistently respecting and valuing others;
- complying with ORGANISATION's policies and procedures;
- using ORGANISATION's resources efficiently and safely;
- taking accountability for their own actions and behaviour;
- demonstrating a duty of care to stakeholders and colleagues;
- maintaining confidentiality;
- avoiding conflicts of interest and declaring them if they arise; and

2 FRAUD CONTROL RESOURCING

The table below illustrates the roles and responsibilities of ORGANISATION's staff and governance bodies in controlling fraud risk.

Role	Responsibility
Audit Committee	▪ review ORGANISATION's Fraud Control Plan at least biennially, or if there is a substantial change to ORGANISATION's structure, functions or activities; ▪ review the appropriateness of ORGANISATION's system of risk oversight and management, including whether the process for developing and implementing the ORGANISATION's fraud control arrangements is sound, and there are appropriate processes and systems in place to detect, capture and effectively respond to fraud risks; ▪ review the Fraud Control Plan to ensure ORGANISATION keeps the plan current and focussed on the areas of greatest risk; and ▪ review steps taken by ORGANISATION to implement recommendations contained in internal and external audit reports and in other reviews within agreed timeframes.
Audit Committee Chair	▪ for the reporting of suspected fraudulent activity, as a last resort;

Role	Responsibility
	▪ promptly arrange for instances of suspected fraud to be examined by a suitably qualified person to determine whether a basis exists for further action; ▪ determine the most appropriate option for resolving the matter, including appointment of internal / external investigating officer; and ▪ receive and review all reports of actual or suspected fraud.
CEO	▪ exhibit to staff and clients a genuine and strong commitment to fraud control; ▪ receive information on suspected instances of fraud and reporting to the Board; and ▪ maintain a strong corporate governance and internal control framework.
Corporate Services Manager	▪ promptly arrange for instances of suspected fraud to be examined by a suitably qualified person to determine whether a basis exists for further action; ▪ report all instances of fraud to the CEO and Audit and Assurance Committee; ▪ refer the matter to the AFP for investigation, and the CDPP for prosecution (upon legal advice) and maintain regular contact with the AFP in relation to all referred cases; ▪ regularly update CEO of the progress of referred cases; and ▪ determine the most appropriate option for resolving the matter, including appointment of internal / external investigating officer.
Risk Manager	▪ ensure ORGANISATION staff undertake annual fraud awareness training; ▪ be the primary point of contact for advice to employees and contractors, and for the reporting of suspected fraudulent activity; ▪ maintain an appropriate recording and tracking system for all instances of suspected fraud (fraud register); and ▪ undertake biennial reviews of Fraud Risk Assessments and Fraud Control Plans.
Managers	▪ participate in Fraud Risk Assessment and subsequent reviews; ▪ remain vigilant in identifying potential fraud; and ▪ implement appropriate controls to prevent fraud.
All ORGANISATION staff and contractors	▪ act in a professional manner, promoting ethical practices and complying with all legal obligations, including all relevant policies and procedures; ▪ perform duties with skill, care, diligence, honesty, integrity and impartiality;

Role	Responsibility
	▪ consider risk, including the risk of fraud, when conducting work for ORGANISATION; ▪ assist in the implementation of fraud control strategies and fully participate in activities relating to fraud control; ▪ remain vigilant and report all instances of suspected fraud; ▪ report instances of suspected fraud in accordance with this Fraud Control Plan; ▪ deal with all reports of fraudulent activity professionally and promptly; and ▪ not hinder or impede an investigation and provide every assistance, as required.

Suspected fraud could be a result of breaches to employee code of conduct. ORGANISATION's Employee Code of Conduct refers to administrative remedies in the event of breaches. Refer to Procedures for Managing Allegations of Misconduct by Employees on further roles and responsibilities of ORGANISATION staff in the investigation of Employee Code of Conduct breaches.

3 FRAUD PREVENTION STRATEGIES

3.1 Integrity Framework

ORGANISATION has implemented the following elements to demonstrate its commitment to integrity:

- ethical senior management team, which recognizes the need for establishing and maintaining an ethical culture;
- communication of expected behaviours in the ORGANISATION's Employee Code of Conduct against which staff are assessed as part of performance reviews;
- governance structure that includes an Audit and Assurance Committee to oversee management's actions with respect to internal controls and risk, including the risk of fraud;
- fraud awareness training;
- process for reporting fraud; and
- ORGANISATION Executive sign off annual certification that a compliance framework, including systems, policies and procedures, is in place and operating effectively to ensure compliance with all ORGANISATION legal and regulatory obligations.

3.2 Fraud awareness training program

It is generally accepted that the most cost effective means of preventing, detecting and deterring fraud in any organisation is the establishment and reinforcement of a sound ethical tone with a high level of staff awareness of the risk of fraud and the impact that it would have on its sustainability. It is equally important that awareness training is provided on a regular basis and that it is perceived by staff as an ongoing activity.

Staff should receive fraud awareness training at least annually.

ORGANISATION recognises that the primary purpose of education and training in the area of fraud awareness is to contribute to the prevention and control of fraud by raising the level of awareness amongst managers and staff. The objective is to assist in the identification of potential fraud risks, possible fraudulent practices and to make it very clear that such practices will not be tolerated by ORGANISATION.

3.3 Internal control

It is important that all business process, especially processes that are more susceptible to the risks of fraud, incorporate rigorous internal controls that are adequate, effective, well documented, updated regularly and understood by personnel.

The internal control system is regularly reviewed internally by an outsourced provider, who conducts a program of internal audits overseen by the Audit and Assurance Committee. The internal audit program is developed and updated annually by the auditor in consultation with, and with the final approval of, the Audit and Assurance Committee.

The internal audit program is a risk-based program which is developed in line with ORGANISATION's identified key risks, including fraud risks. This ensures that core priorities and risks are addressed by the internal auditor, in a manner consistent with ORGANISATION's risk profile and tolerance to each area of risk.

ORGANISATION financial statements and controls related to these are externally audited by an independent organisation. In additional, ORGANISATION is quality accredited, assessed under the QIC Health and Community Services Standards.

3.4 Fraud risk assessments

A key element in preventing the risk of fraud is to regularly conduct a fraud risk assessment. The process of conducting a fraud risk assessment includes:

- understanding the risks facing the organisation;
- identifying the existing controls in place to mitigate the risk of fraud;
- assessing the risk of fraud in terms of its consequence and likelihood to rate each risk;
- identifying risk treatments if the risk rating is above acceptable fraud risk; and
- assessing if the level of target risk of fraud facing the organisation (post-risk treatment) is acceptably low.

Risk rating tables articulating the criteria for making assessments of the likelihood and consequence of risks eventuating are documented in **Appendix A**.

The risk of fraud is to be formally assessed at least every two years, or when there's a substantial change to ORGANISATION's structure, functions or activities.

The 2019 Fraud Risk Assessment is included in **Appendix B**. The Fraud Risk Assessment details the identified fraud risks, controls in place, and assessments of likelihood and consequence leading to a rating for each risk.

The overall fraud risk of ORGANISATION is assessed as **XXXX.** Generally, the fraud controls in place are regarded as adequate and management and ORGANISATION's Audit and Assurance Committee should continue to monitor and test the operating effectivness of the specific operation of those controls to ensure that they continue to meet both current and emerging risks.

It should be noted that this assessment is based on the adequacy of the controls that are currently in place and risk treatments which will be implemented. The effectiveness of these internal controls needs to be maintained to minimise incidences of fraud and maintain or improve on this assessment. Risk treatments need to be implemented and assessed for adequacy and effectiveness. ORGANISATION management and the Audit and Assurance Committee are responsible for continuing to monitor the specific operation of those controls to ensure that they continue to meet both current and emerging risks.

Additional controls should be identified for risks that are assessed as 'high' or 'extreme'. No fraud risks rated as 'high' or 'extreme' were identified.

4 FRAUD DETECTION STRATEGIES

4.1 Fraud detection program

Detection systems are implemented with the aim of detecting fraud, in the event preventative systems fail. Detection systems implemented by ORGANISATION operate in conjunction with preventative systems. ORGANISATION's detection systems include:

- post-transactional reviews such as bank reconciliations, travel reconciliations, credit / travel card acquittals;
- computer system analysis such as a review of audit logs; and
- analysis of management accounting reports to identify trends

4.2 Defining the External Auditor's role in the detection of fraud

ORGANISATION's financial statements audit is undertaken by an independent external organisation, which assigns staff who have the necessary skills and experience to undertake this work. External auditors have a responsibility to undertake audit procedures which increase the likelihood of detecting a material misstatement in financial statements due to fraud (or error)[1]. The external auditors attend the Audit and Assurance Committee meetings and provides updates on issues encountered during the phases of external audit, which will include any suspected instances of fraud.

4.3 Mechanisms for reporting suspected fraud incidents

Staff are the 'eyes and ears' of any organisation. They are, consequently, key to the prevention, detection and deterrence of fraud in ORGANISATION. It is important that staff be provided with the

[1] 'Role of the External Auditor in the detection of fraud', in *AS 8001-2008 Fraud and Corruption Control*, Standards Australia, 2008, p 45

information necessary to identify and make timely reports of instances of potential fraud risks or incidents involving suspicion of fraud.

The organisation outlines the following simple steps for staff to follow in a situation where they face an alleged or suspected fraudulent activity that they would like to report:

Note concerns and observations	▪ do not jump to conclusions; ▪ carefully observe and note the suspected conduct; ▪ document your own actions; and ▪ keep any documents as possible evidence and do not alter them.
Report concerns	▪ report all cases of suspected fraud to the General Manager Finance & Corporate and/ or the Deputy CEO who is available to provide advice on a confidential basis; and ▪ information on the identity of someone reporting fraud is strictly confidential and will not be released to other ORGANISATION staff without the consent of the complainant.
Inform only persons who need to know and maintain confidentiality	▪ to prevent possible destruction of evidence by persons involved; ▪ as protection against undue pressure from those at the centre of any allegations; and ▪ to protect the rights of the person suspected of the fraudulent activity who may, in fact, be innocent.

Prompt reporting of suspected instances of fraud is key to the successful detection of offender(s) and the limiting of loss to resources and/or damage to ORGANISATION's reputation.

5 RESPONDING TO DETECTED FRAUD INCIDENTS

This section provides guidance to ORGANISATION staff and decision makers if a fraud incident occurs and should be read in conjunction with the Fraud Response Diagram included at **Appendix C**.

5.1 Reporting instances of fraud

Suspected fraud should be reported to the General Manager Finance & Corporate or Deputy CEO in the first instance. Suspected fraud should be reported to the Audit and Assurance Committee Chair only as a last resort.

A fraud register should be maintained and include the following information on reported instances:

- date and time of report;

- date and time that incident was detected;
- how the incident came to the attention of management (e.g. anonymous report, normal report, supplier report);
- the nature of the incident;
- value of loss to ORGANISATION; and
- action taken following discovery of the incident.

5.2 Initial assessment

The (Insert responsible Staff position) will promptly arrange for instances of suspected fraud to be examined by a suitably qualified person to determine whether a basis exists for further action. That is, if the nature of the allegation is a potential fraud or misconduct only. If determined that the reported incident is a potential fraud, preliminary investigation is initiated.

Every instance will be reported to the ORGANISATION CEO and reported to the Board, and Audit and Assurance Committee.

5.3 Preliminary investigation

The preliminary investigation will determine whether an incident of alleged fraud is sufficiently serious or complex to be referred to the AFP for investigation. In determining whether an incident of alleged fraud should be referred to the AFP, ORGANISATION will:

- conduct a preliminary investigation of the alleged incident;
- satisfy itself that there is reasonable cause to believe an offence has been committed or attempted;
- verify that the matter is of a fraudulent nature within the terms of the definition of fraud; and
- check that the offence, or attempted offence is serious or complex.

If it is determined that a serious or complex fraud is likely to have been committed, the General Manager Finance & Corporate / Deputy CEO may refer the matter to the AFP for investigation, and the CDPP for prosecution (upon legal advice). Any criminal activity is also to be referred to the AFP.

5.4 Fraud investigation procedures

The following is presented for the information of ORGANISATION staff that may be given a role in conducting investigation of a suspected fraudulent activity.

5.4.1 AFP investigation

If the AFP agrees to take on the referred case, they will undertake the investigation and follow on action as necessary. The General Manager Finance & Corporate / Deputy CEO is to maintain regular contact with the AFP in relation to all referred cases. The ORGANISATION CEO will be regularly updated of the progress of referred cases.

5.4.2 Internal investigation

If the AFP rejects the matter for investigation or if ORGANISATION decides not to refer a matter to the AFP, the (insert responsible Staff Position), is to determine the most appropriate option for resolving

the matter. In these circumstances, ORGANISATION may consider taking no further action or initiating further investigations internally (or with external assistance) to determine the following:

- no further action;
- criminal prosecution;
- civil proceedings; and
- imposing penalties under the Code of Conduct.

If the AFP declines to investigate a potential offence and returns the matter, ORGANISATION may, if it has investigated the matter and obtained sufficient evidence during its referral submission to the AFP, subsequently refer the matter to the Commonwealth Department of Public Prosecution (CDPP) for consideration of prosecution action.

5.4.3 Qualifications for staff involved in fraud investigation

Investigations should be carried out by appropriately qualified and experienced personnel with the appropriate level of managerial oversight. If external investigators are engaged, they should also be appropriately qualified and supervised.

5.5 Response

ORGANISATION is responsible for making decisions at a number of critical stages in the management of a suspected fraud, including subsequent decisions on the actions resulting from an investigation, such as referral of a brief of evidence to the CDPP, or application of administrative, disciplinary or civil sanction or other action (such as a decision to take no further action).

Status and results of all investigations should be reported to ORGANISATION's Audit and Assurance Committee.

5.5.1 Proceed with prosecution

On completion of the fraud investigation, collection and collaboration of available evidence and preparation of a brief of evidence, ORGANISATION can consider whether prosecution is appropriate. ORGANISATION should consult the Australian Government's policy on prosecution of criminal offences, which is set out in the *Prosecution Policy of the Commonwealth*, and available on the CDPP website.[2]

The *Prosecution Policy* provides a two-stage test that must be satisfied before a prosecution is commenced:

- there must be sufficient evidence to prosecute the case; and
- it must be evident from the facts of the case, and all the surrounding circumstances, that the prosecution would be in the public interest.

Once ORGANISATION has concluded that sufficient evidence is available and prosecution would be in in the public interest, submission of the prepared brief of evidence can be made to the CDPP.

5.5.2 Proceed with civil remedies

If ORGANISATION sends a brief of evidence to the CDPP to consider prosecution action, and the CDPP advises that a prosecution will not proceed, ORGANISATION remains responsible for resolving the

[2] https://www.cdpp.gov.au/sites/default/files/Prosecution-Policy-of-the-Commonwealth_0.pdf

matter and for considering other available remedies. Civil proceedings may be a means to remedy a wrong for which a lower standard of proof is required.

5.5.3 Proceed with administrative remedies

If the evidence cannot establish the degree of intention, recklessness or negligence required for a criminal offence, or if the matter is trivial, it may be appropriate to apply administrative remedies detailed in the Procedures for Managing Alleged Misconduct by Employees, as referenced in ORGANISATION's Employee Code of Conduct.

5.6 Resolution

5.6.1 Recovery of money or property lost through fraud

ORGANISATION will take all reasonable measures to recovering financial losses caused by illegal activity through proceeds of crime and civil recovery processes or administrative remedies. Actions to be taken will be determined following an assessment of the costs and benefits of recovering such losses and the likelihood of recovery.

5.6.2 Review of internal controls

In each instance where fraud is detected, senior management and line management will reassess the adequacy and effectiveness of ORGANISATION's internal control environment and assess if improvements are required. Where improvements are necessary, these will be implemented as soon as practicable.

6 WHISTLEBLOWING POLICY

The *Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2018* is introducing amendments to the *Corporations Act 2001* that require all public companies and large proprietary companies have a whistleblower policy. The requirements of the policy are outlined in section 1317AI (5), including:

a) information about the protections available to whistleblowers, including protections under Part 1317AI
b) information about to whom disclosures that qualify for protection under Part 1317AI may be made, and how they may be made
c) information about how the company will support whistleblowers and protect them from detriment
d) information about how the company will investigate disclosures that qualify for protection under Part 1317AI
e) information about how the company will ensure fair treatment of employees of the company who are mentioned in disclosures that qualify for protection under Part 1317AI, or to whom such disclosures relate
f) information about how the policy is to be made available to officers and employees of the company
g) any matters prescribed by the regulations for the purposes of this paragraph.

Appendix A – Risk Rating Tables

Risk Impact Category

The risk impact categories listed below provide examples of possibilities to assist with risk identification and identify key drivers and underlying causes.

Risk Impact Category			
Financial	Resources	Safety/WHS	Environment / heritage
Information management	Reputation	Legal	Stakeholders
Service delivery	Security / compliance		

Assessing Likelihood

The likelihood is the chance of something happening. When assessing the likelihood takes into account the effectiveness of controls that currently exist. The following table provides guidance when determining the likelihood of an event happening.

Rating	Likelihood	Criteria
Almost certain	Almost certain will occur	>75%
Likely	More likely to occur than not	51-75%
Possible	Fairly likely to occur	26-50%
Unlikely	Unlikely to occur	6-25%
Rare	Extremely unlikely or virtually impossible	0-5%

Assessing Risk Ratings

After assessing a risk's likelihood and consequence, the following table is used to assess the risk rating.

Rating	**Consequences**				
Likelihood	**Insignificant**	**Minor**	**Moderate**	**Major**	**Extreme**
Almost Certain	Low	Medium	High	Severe	Severe
Likely	Low	Low	Medium	High	Severe
Possible	Low	Low	Medium	Medium	High
Unlikely	Very Low	Low	Low	Medium	High
Rare	Very Low	Very Low	Low	Low	Medium

Assessing Consequences

The consequence is the outcome of an event (risk) affecting objectives.

The table below describes the ratings that can be selected to determine how severe the consequence or impact would be if a risk occurs.

Impact Description	**Consequence Rating**				
	Extreme	**Major**	**Moderate**	**Minor**	**Insignificant**
Financial	Net loss impacting the organisation's financial position by greater than $1.5m.	Net loss impacting the organisation's financial position between $0.5m and $1.5m.	Net loss impacting the organisation's financial position between $0.25m and $0.5m.	Net loss impacting the organisation's financial position between $50,000 and $250,000.	Insignificant impact on the organisation's net financial position

Impact Description	Consequence Rating				
	Extreme	Major	Moderate	Minor	Insignificant
Financial (continued)	Establishing an indemnity exceeding $20m which is not approved.	Establishing an indemnity exceeding $20m which is approved.	Establishing an indemnity of $5-$20m	Establishing an indemnity which is below $5m.	involving less than $50,000.
Resources	Destruction/loss or permanent impairment of significant organisation's assets. Incident causes a significant reduction in staff retention and recruitment.	Destruction/loss of a large proportion of the organisation's assets. Skilled staff shortages leads to significant additional cost.	Damage to, or other impairment of, a significant proportion of assets. Skilled staff shortages leads to moderate additional cost.	Damage to, or other impairment of, a small proportion of assets. Staff absences increase sufficiently to cause delays.	Loss or reparable damage to small number of assets. Insignificant impact on targets.
Safety and WHS	Multiple fatalities and/or irreversible disability or impairment of numerous people.	A single fatality, or extensive injuries, irreversible disability or impairment to multiple people. Medium term, largely reversible disability to one or more persons. Medical treatment required for one or more persons.	Medium term, largely reversible disability to one or more persons. Medical treatment required for one or more persons.	Minor injuries or ailments. First aid treatment required.	Insignificant injury or ailment, no treatment required
Environment and heritage	Destruction or serious permanent damage to significant heritage or environment resources.	Major detrimental damage to heritage or environment resources or long-term effects.	On-site environmental releases contained with outside assistance, medium-term environmental effects. Moderate damage to heritage resources.	Minor environmental impacts, any environmental on-site releases or heritage resources damages are contained.	Insignificant effects on heritage or environment assets.

Impact Description	Consequence Rating				
	Extreme	Major	Moderate	Minor	Insignificant
Information Management	Severe loss or corruption to the majority of critical information systems and resources (including IT-based and other significant records) severely impacting business continuity for a prolonged period. Critical loss of corporate knowledge through unavailability of key personnel.	Loss or irrecoverable corruption of critical or significant information systems and resources impacting business continuity for a period. Major loss of corporate knowledge through unavailability of key personnel.	Corruption of key information systems and resources (including personnel) impacting operations.	Disruptions or corruption of routine 'administrative' information resources.	Insignificant disruptions, loss or impairment of small amount of administrative information.
Reputation	National public outrage or condemnation and high-level political criticism (resulting in government inquiry). Includes sustained adverse media attention or public outcry, across multiple media channels. Loss of confidence and/or support from major stakeholders.	Local public outrage or condemnation and local political criticism (resulting in inquiry). Includes adverse media attention or public outcry, across multiple media channels.	Adverse local media attention or criticism from a recognised segment of the community.	Local media enquiries and minor reporting. Criticism from minor community segment.	Insignificant public or media attention.
Legal	Breaches of legislation or regulatory requirements with severe	Breaches of legislation or regulatory requirements with major consequences	Breaches of legislation or regulatory requirements with	Breaches of legislation or regulatory requirements with	Breaches of legislation or regulatory requirements with insignificant

Impact Description	Consequence Rating				
	Extreme	Major	Moderate	Minor	Insignificant
	consequences such as prosecutions, major litigation and severe fines.	such as litigation and/or major fines.	moderate consequences such as investigations, threat of litigation, moderate fines and/or additional reporting.	minor consequences such as minor legal issues and/or fine imposed.	consequences and/or breaches of regulations.
Stakeholders	Severe Commonwealth (and/or Local) government, public / community effects or social issues, resulting in complete loss of confidence and support for the organisation and being unable to deliver its outcomes.	Major government, public/community effects or social issues, resulting in significant loss of confidence and support in the organisation.	Moderate adverse government, public/community effects or social issues, resulting in concerns around specific actions or outcomes.	Local concern or criticism from government, public/community or social matters with minor impact.	Insignificant government, public/community or social impacts.

Impact Description	Consequence Rating				
	Extreme	Major	Moderate	Minor	Insignificant
Service delivery	Impact to multiple and diverse areas of the organisation, threatening viability of the organisation. Executive intervention necessary, with mobilisation of resources including external assistance. Destruction or serious damage to key physical or information assets Would threaten survival of the organisation.	May require senior management intervention May require external assistance. Unavailability of staff, damage to physical assets; major loss of productivity due to IT disruption. Disruption (up to one month) to operations. Would threaten the effective function of a program/project.	Impact to multiple areas of the organisation. Substantial management support required to resolve local issue. Temporary loss of key staff Minor service interruption (e.g. power failure, floods) across the organisation. Some disruption (up to one day) to operations manageable by altered operational routine.	Minor staff impact, minor/localised interruption to premises; minor / isolated service interruption. Local management intervention required with locally available resources. Manageable by local intervention.	Insignificant impact, no measurable operational delay or interruption. No management intervention required and managed by local staff.
Security and compliance	Security incident causes death and destruction. Security incident compromises the integrity of critical IT infrastructure.	Permanent disability to staff/clients because of improper work practices. Undetected long-term fraud (discovered by accident rather than process). Sensitive information leaks.	Failure to comply with directions and instructions Systemic fraud of significant value.	Security systems or processes not being adhered to.	Failure to comply with internal instructions.

Appendix B – ORGANISATION Fraud Risk Assessment Examples – will need to be modified for particular organisation

Risk no.	The fraud risk (description)	Factors or Source of Risk	Impact	Existing Key Controls	Current Risk (accounting for existing key controls)		Is the risk rating acceptable?	Risk Treatment	Target Risk (after treatment)	
					Assessment	Risk Rating			Assessment	Risk Rating
1	*Cyber security fraud:* *An event of cyber security fraud may include the following:* • *Threats from malicious software (viruses, spyware, worms etc.) introduced into the ORGANISATION's IT environment.* • *Unauthorised access to, and use of, ORGANISATION systems and information.* • *ORGANISATION staff receiving scam emails demanding payment.* • *ORGANISATION staff receiving ransomware (malicious software designed to block access to a computer system until a sum of money is paid).* • *Hacking into ORGANISATION systems to access personnel information.*	• *Security control measures are inadequate for ORGANISATION's needs* • *Physical security measures are inadequate or out of date* • *Reported incidents are not completed or addressed* • *Lack of training & awareness around ICT security*	• *Financial* • *Reputation* • *Information management* • *Security and compliance*	•						
2	*Misuse of ORGANISATION Branding and Name* • *Individuals misrepresent their views as being those of ORGANISATION.* • *Individuals use ORGANISATION branding to imply nonexistent relationships to gain financial or other advantage.*	• *Use of ORGANISATION merchandise to further personal / financial interests* • *Desire to use ORGANISATION brand as a conduit to specific organisations / govt agencies* • *Disgruntled staff obtaining confidential or incorrect information and distributing to the public under the ORGANISATION brand*	• *Reputation* • *Legal* • *Stakeholders*	•				•		
3	*False representation in recruitment:* *False representations of qualifications, professional accreditations, skills, experience, employment history or heritage to obtain employment or appointment.*	• *Overriding or inadequate controls* • *Applicants intentionally submit fraudulent representations in the application process* • *High staff turnover*	• *Reputation* • *Financial* • *Resources*	•				•		

Risk no.	The fraud risk (description)	Factors or Source of Risk	Impact	Existing Key Controls	Current Risk (accounting for existing key controls)		Is the risk rating acceptable?	Risk Treatment	Target Risk (after treatment)	
					Assessment	Risk Rating			Assessment	Risk Rating
4	*Fraudulent use of credit cards:* *Corporate credit/travel card misuse and travel & entertainment claims (including internal and external fraud).* • *Cards are issued to fictitious employees or persons.* • *Cards are issued to / used by persons outside the organisation whom obtain a ORGANISATION credit card (or card number).* • *Credit card number, bank account and or other in-confidence information is used by staff or others for unauthorised purposes (e.g. to make purchases on the internet).*	• *Credit card acquittal process is not performed.* • *Credit card holders are not fully aware of ORGANISATION policies and procedures on credit cards* • *Issue of corporate credit/travel card to unauthorised person.* • *Credit card acquittal process is not performed.* • *Credit card acquittal process is not reviewed / approved.*	• *Financial* • *Reputation*	•						
5	*Non- declaration of conflict of interest by Board Members and other ORGANISATION Stakeholders*	• *Misusing authority to benefit own or related interests*	• *Reputation* • *Financial*					•		
6	*Supplier fraud:* *Fraudulent activity by external suppliers may include:* • *Charging in excess of agreed price* • *Charges for which no goods are received, personal purchases, or goods of less quality / quantity than that contractually required* • *Deliberate duplicate invoices* • *Payments to fictitious companies.*	• *Lack of independent market testing* • *Inadequate checking of invoices to contracts* • *System failure allowing fraudulent use/manipulation of records.* • *Contracts contain insufficient penalties for poor performance.*	• *Financial*	•						
8	*Theft of ORGANISATION assets:* *An employee or external party intentionally steals assets owned and controlled by ORGANISATION or an employee falsely claiming a ORGANISATION asset as lost or stolen. Assets include IT assets, physical assets and portable and attractive (P&A) items* *Failure to return ORGANISATION assets upon ceasing employment.*	• *Poor internal controls around monitoring and tracking of assets* • *Register of assets issued to individuals is not kept up to date* • *Lack of segregation of duties*	• *Financial* • *Resources*	•						
9	*Override of IT controls by superuser:* *Unauthorised use / disclosure of commercially sensitive, confidential or personal information that is of value to third parties.*	• *IT manager having superuser access and able to obtain information without authorisation*	• *Information management* • *Security / compliance* • *Reputation*	•						

Risk no.	The fraud risk (description)	Factors or Source of Risk	Impact	Existing Key Controls	Current Risk (accounting for existing key controls)		Is the risk rating acceptable?	Risk Treatment	Target Risk (after treatment)	
					Assessment	Risk Rating			Assessment	Risk Rating
10	*Leave entitlements fraud (AL, LSL, Carers, Flex, Toil):* • *Leave taken not being entered into the system.* • *Leave supported by false or misleading medical evidence.* • *Flex/timesheet falsification.*	• *Overriding or inadequate controls* • *System failure allowing fraudulent use or manipulation of flex sheet and leave applications* • *Low staff morale* • *Complicated systems becoming a deterrent to staff being accurate in their timesheets*	• *Financial* • *Resources*	•						
11	*Fraudulent travel:* • *Travelling at ORGANISATION when not required for business purposes* • *Travel booked and travel allowance claimed but travel not undertaken.*	• *Travel offers opportunity to see other sites/events* • *Additional income from travel allowances*	• *Financial* • *Resources*	•						

Appendix C – Fraud Response Diagram